G. PARMEGGIANI 26/2/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)
Corso di Laurea: Informatica

PRESENTAZIONE DEL CORSO (nel file: INFORMAT.pdf)

DIVISIONE NEI NUMERI NATURALI E NEI NUMERI INTERI

Siano

$\mathbb{N}$ = l'insieme dei NUMERI NATURALI = $\{0,1,2,3,4,\dots\}$

$\mathbb{Z}$ = l'insieme dei NUMERI INTERI = $\{\dots,-4,-3,-2,-1,0,1,2,3,4,\dots\}$

DIVISIONE IN $\mathbb{N}$: Siano $a,b \in \mathbb{N}$ con $b \neq 0$. Allora ESISTONO e SONO UNICI due numeri naturali

q (detto QUOZIENTE) ed
r (detto RESTO) tali che

$$a = b \cdot q + r \quad \text{con} \quad (0 \leq)\, r < b$$

($r \in \mathbb{N}$ quindi $r \geq 0$)

ESEMPIO 1

$a = 137$
$b = 55$

$$\underset{a}{137} = \underset{b}{55} \cdot \underset{q}{\boxed{2}} + \underset{r}{\boxed{27}}$$

N.B. $0 \leq 27 < 55$

ESEMPIO 2

$a = 137$
$b = 142$

$$\underset{a}{137} = \underset{b}{142} \cdot \underset{q}{\boxed{0}} + \underset{r}{\boxed{137}}$$

N.B. $0 \leq 137 < 142$

NB1 L'ESISTENZA di q ed r può essere dimostrata usando il PRINCIPIO DI INDUZIONE

NB2 che q ed r siano UNICI significa:

$$\left.\begin{aligned} a &= b\cdot q_1 + r_1 \quad \text{con } 0 \le r_1 < b \\ a &= b q_2 + r_2 \quad \text{con } 0 \le r_2 < b \end{aligned}\right\} \Rightarrow \begin{cases} q_1 = q_2 \\ r_1 = r_2 \end{cases}$$

DIVISIONE IN $\mathbb{Z}$: Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Allora

ESISTONO e SONO UNICI due numeri interi

q (detto **QUOZIENTE**) e

r (detto **RESTO**) tali che

$$a = b\cdot q + r \quad \text{CON} \quad 0 \le r < |b|$$

NB3 se non si impone la condizione $0 \le r < |b|$, non si ha l'unicità di q ed r.

ESEMPIO 1

$a = 137$

$b = -55$

ALLORA: $\underbrace{137}_{a} = \underbrace{(-55)}_{b} \cdot \underbrace{\boxed{(-2)}}_{q} + \underbrace{\boxed{27}}_{r}$

MA ANCHE $\underbrace{137}_{a} = \underbrace{(-55)}_{b} \cdot (-3) + (-28)$

ATTENZIONE: Prenderemo q ed r nella divisione in cui $0 \le r < |b|$ (quindi qui $q = -2$ ed $r = 27$)

ESEMPIO 2

$a = -137$

$b = 55$

$$-137 = 55 \cdot q + r$$

1) non può essere $q \ge 0$ perché, se lo fosse, da $r \ge 0$ e $55 > 0$ seguirebbe che anche $55 \cdot q + r \ge 0$ (mentre $-137 < 0$)

QUINDI $q<0$

2) non può essere $q=-1$: se lo fosse da

$-137 = 55 \cdot q + r$ si otterrebbe

$-137 = -55 + r$ e quindi $r<0$ (mentre $r \geq 0$)

3) non può essere $q=-2$: se lo fosse da

$-137 = 55 \cdot q + r$ si otterrebbe

$-137 = -110 + r$ e quindi $r<0$ (mentre $r \geq 0$)

$\Rightarrow$ va bene $q=-3$:

$$\underbrace{-137}_{a} = \underbrace{55}_{b} \underbrace{\boxed{(-3)}}_{q} + \underbrace{\boxed{28}}_{r}$$

N.B. $0 \leq 28 < 55$

[4) non può essere $q<-3$: prendendo $q<-3$ si otterrebbe sì $r \geq 0$, ma anche $r > |b| = 55$ (mentre si richiede $0 \leq r < |b|$]

NB1 La dimostrazione dell'ESISTENZA di q ed r è simile alla dimostrazione dell'esistenza del quoziente e del resto nella divisione in $\mathbb{N}$

NB2 Che q ed r siano UNICI segue dalla richiesta

$$0 \leq r < |b|$$

NB3 Se $a, b \in \mathbb{Z}$ con $b \neq 0$, allora $|a|, |b| \in \mathbb{N}$ con $|b| \neq 0$, ma non c'è nesso tra il quoziente ed il resto della divisione di a con b ed i valori assoluti del quoziente e del resto della divisione di $|a|$ con $|b|$.

ESEMPIO $a = -137$
$b = 55$

DIVISIONE IN $\mathbb{Z}$: $$\underbrace{-137}_{a} = \underbrace{55}_{b} \cdot \underbrace{\boxed{(-3)}}_{q} + \underbrace{\boxed{28}}_{r}$$

$|a| = 137 \in \mathbb{N}$

$|b| = 55 \in \mathbb{N}$

$$\underbrace{137}_{|a|} = \underbrace{55}_{|b|} \cdot 2 + \boxed{27}$$

← questo NON è $|28|$

questo non è $|-3|$

PER CASA: ESERCIZIO 1 (file: I19casaT1.pdf)

DIVISIBILITÀ NEI NUMERI NATURALI E NEI NUMERI INTERI

DIVISIBILITÀ IN $\mathbb{N}$: siano $a, b \in \mathbb{N}$ con $b \neq 0$. Si dice che

b DIVIDE a se

$$a = b \cdot q \quad \text{per un opportuno } q \in \mathbb{N}.$$

Se b DIVIDE a si scrive $b | a$

Se b NON DIVIDE a si scrive $b \nmid a$

ESEMPI $6 | 18$ infatti $18 = 6 \cdot q$ (con $q \in \mathbb{N}$: si prenda $q = 3$)

$4 \nmid 18$ infatti nella divisione di 18 per 4 c'è un resto $r \neq 0$

$(18 = 4 \cdot q + r$ con $q = 4$ e $r = 2 \neq 0)$

NB Siano $a, b \in \mathbb{N}$ con $a \neq 0$ e $b \neq 0$. Allora

$$\left.\begin{array}{l} a | b \\ b | a \end{array}\right\} \Longrightarrow a = b$$

DIVISIBILITÀ IN $\mathbb{Z}$: siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Si dice che

b DIVIDE a se

$$a = q \cdot b \quad \text{per un opportuno } q \in \mathbb{Z}.$$

se **b DIVIDE a** si scrive $b \mid a$

se **b NON DIVIDE a** si scrive $b \nmid a$

ESEMPI

$(-6) \mid 18$ perché esiste $q \in \mathbb{Z}$ tale che $18 = q \cdot (-6)$
(si prenda $q = -3$)

$6 \mid (-18)$ perché esiste $q \in \mathbb{Z}$ tale che $-18 = q \cdot 6$
(si prenda $q = -3$)

$4 \nmid (-18)$: nella divisione di -18 per 4 c'è un resto $r \neq 0$
(nella divisione di -18 per 4, dovendo essere $r \geq 0$
è $q = -5$ ed $r = 2$)

NB se $a, b \in \mathbb{Z}$ con $a \neq 0$ e $b \neq 0$

$$\left.\begin{array}{l} a \mid b \\ b \mid a \end{array}\right\} \Rightarrow a \in \{b, -b\}$$

MASSIMO COMUN DIVISORE NEI NUMERI NATURALI E NEI NUMERI INTERI

MASSIMO COMUN DIVISORE IN $\mathbb{N}$:

Siano $a, b \in \mathbb{N}$ **NON ENTRAMBI NULLI**. Si dice che $d \in \mathbb{N}$ è UN massimo comun divisore di a e b se

1) $d \mid a$ e $d \mid b$ (ossia se d è un divisore comune di a e b)

2) se $z \mid a$ e $z \mid b$ per qualche $z \in \mathbb{N}$, allora $z \mid d$
(ossia se d è un multiplo di tutti i divisori comuni di a e b)

NB2 In $\mathbb{N}$ il massimo comun divisore è UNICO

NB1 In $\mathbb{N}$ il massimo comun divisore è UNICO

(ossia se $a, b \in \mathbb{N}$ sono non entrambi nulli d_1 e d_2 sono due divisori comuni di a e b con la proprietà di essere multipli di ogni altro divisore comune di a e b, allora $d_1 = d_2$).

Se d è IL massimo comun divisore di a e b (in $\mathbb{N}$) si scrive

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

ESEMPIO $6 = MCD(12, 18)$

NB2 Siano $a, b \in \mathbb{N}$ non entrambi nulli. Allora

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

NB3 Siano $a, b \in \mathbb{N}$ con $b \neq 0$,

SE $b | a$ ALLORA $b = MCD(a, b)$

In particolare, per ogni $b \neq 0$ si ha che

$$b = MCD(0, b) = MCD(b, 0).$$

NB4: Siano $a, b \in \mathbb{N}$ con $b \neq 0$. Siano q ed r il quoziente ed il resto della divisione di a per b (con eventualmente $r = 0$ se $b | a$)

$$a = b \cdot q + r \quad \text{con} \quad 0 \leq r < b.$$

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

perché $\left.\begin{array}{l} a=bq+r \\ d|a \\ d|b \end{array}\right\} \Rightarrow d|r$

per cui $\{d \mid d$ divisore comune di a e $b\} \subseteq \{d \mid d$ divisore comune di b e $r\}$

e viceversa $\left.\begin{array}{l} a=bq+r \\ d|b \\ d|r \end{array}\right\} \Rightarrow d|a$

per cui anche

$\{d \mid d$ divisore comune di b e $r\} \subseteq \{d \mid d$ divisore comune di a e $b\}$

MASSIMO COMUN DIVISORE IN $\mathbb{Z}$:

Siano $a, b \in \mathbb{Z}$ NON ENTRAMBI NULLI. Si dice che $d \in \mathbb{Z}$ è UN massimo comun divisore di a e b se

1) $d|a$ e $d|b$ (ossia d è un divisore comune di a e b)

2) se $z|a$ e $z|b$ per qualche $z \in \mathbb{Z}$, allora $z|d$
   (ossia d è un multiplo di tutti i divisori comuni di a e b).

Se d è UN massimo comun divisore di a e b (in $\mathbb{Z}$) si scrive

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

ESEMPI

$6 = MCD(12,18)$ ma anche

$-6 = MCD(12,18)$ in $\mathbb{Z}$

$6 = MCD(-12,18)$ ma anche

$-6 = MCD(-12,18)$

NB1 In $\mathbb{Z}$ il massimo comun divisore è individuato a meno del segno (ossia se $a, b \in \mathbb{Z}$ sono non entrambi nulli, e $d_1, d_2 \in \mathbb{Z}$ sono due divisori comuni di a e b con la proprietà di essere multipli di ogni altro divisore comune di a e b, allora $d_1 = d_2$ oppure $d_1 = -d_2$)

NB2 Siano $a,b \in \mathbb{Z}$ con $b \neq 0$. Siano q ed r il quoziente ed il resto della divisione di a per b (con eventualmente $r=0$ se $b|a$):

$$\boxed{\begin{array}{l} a = b \cdot q + r \quad \text{con} \quad 0 \leq r < |b| \\ \text{ALLORA} \quad MCD(a,b) = MCD(b,r) \end{array}}$$

NB3 Siano $a,b \in \mathbb{Z}$ non entrambi nulli. Allora

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

ESEMPIO in $\mathbb{Z}$ $\quad MCD(-12,8) = MCD(12,8)$

e $d = MCD(-12,8) \Longleftrightarrow d \in \{4,-4\}$

CALCOLO DEL MASSIMO COMUN DIVISORE IN $\mathbb{N}$

Dati $a,b \in \mathbb{N}$ con $a \neq 0$ e $b \neq 0$, descriviamo un algoritmo (detto **ALGORITMO DI EUCLIDE**) che permette di calcolare $MCD(a,b)$. Esso consiste in una sequenza di divisioni successive:

1° PASSAGGIO: si divide a per b: $\exists\, q_1, r_1 \in \mathbb{N}$ tali che

$$a = b \cdot q_1 + r_1 \quad \text{con} \quad 0 \leq r_1 < b$$

$$MCD(a,b) = MCD(b,r_1)$$

$\boxed{\text{SE } r_1 = 0}$ allora $MCD(b,r_1) = MCD(b,0) = b$ e l'algoritmo si ferma: $MCD(a,b) = b$

$\boxed{SE\ r_1 \neq 0}$ l'algoritmo continua

ESEMPIO 1

$MCD(36,12) = \dots$

$$\underbrace{36}_{a} = \underbrace{12}_{b} \cdot \underbrace{3}_{q_1} + \underbrace{0}_{r_2}$$

$r_1 = 0 \Rightarrow b | a \Rightarrow MCD(a,b) = b$

$MCD(36,12) = 12$

ESEMPIO 2

$MCD(42,12) = \dots$

$$\underbrace{42}_{a} = \underbrace{12}_{b} \cdot \underbrace{3}_{q_1} + \underbrace{6}_{r_1}$$

$r_1 \neq 0 \Rightarrow$ CONTINUO

2° PASSAGGIO se $r_1 \neq 0$, si divide b per r_1:

$\exists q_2, r_2 \in \mathbb{N}$ tali che

$$b = r_1 \cdot q_2 + r_2 \quad \text{con} \quad 0 \leq r_2 < r_1$$

$$MCD(b, r_1) = MCD(r_1, r_2)$$

$\boxed{SE\ r_2 = 0}$ allora $MCD(r_1, r_2) = MCD(r_1, 0) = r_1$

e l'algoritmo si ferma:

$$MCD(a,b) = MCD(b,r_1) = MCD(r_1,r_2) = r_1$$

$\boxed{SE\ r_2 \neq 0}$ l'algoritmo continua

DALL' ESEMPIO 2 ...

DALL' ESEMPIO 2 ...

$MCD(42,12) = \ldots$

1° PASSAGGIO : $\underbrace{42}_{a} = \underbrace{12}_{b} \cdot \underset{q_1}{3} + \underset{r_1}{6}$ $\quad r_1 \neq 0 \Rightarrow$ continuo

2° PASSAGGIO : $\underbrace{12}_{b} = \underbrace{6}_{r_1} \cdot \underset{q_2}{2} + \underset{r_2}{0}$

$\left.\begin{array}{l} r_2 = 0 \\ r_1 \neq 0 \end{array}\right\} \Rightarrow MCD(42,12) = r_1 = 6$

... se $r_2 \neq 0$ l'algoritmo continua e

IL MASSIMO COMUN DIVISORE $MCD(a,b)$ E' L'ULTIMO RESTO NON NULLO DELLA SEQUENZA DI DIVISIONI SUCCESSIVE

ESEMPIO 1 $\quad MCD(36,28) = \ldots$

1° PASSAGGIO $\quad \underbrace{36}_{a} = \underbrace{28}_{b} \cdot \underbrace{1}_{q_1} + \underbrace{8}_{r_1}$ $\quad r_1 \neq 0 \Rightarrow$ continuo

⋮

2° PASSAGGIO $\quad \underbrace{28}_{b} = \underbrace{8}_{r_1} \cdot \underbrace{3}_{q_2} + \underbrace{4}_{r_2}$ $\quad r_2 \neq 0 \Rightarrow$ continuo

3° PASSAGGIO $\quad \underbrace{8}_{r_1} = \underbrace{4}_{r_2} \cdot \underbrace{2}_{q_3} + \underbrace{0}_{r_3}$

$$\left.\begin{array}{l} r_3 = 0 \\ r_2 \neq 0 \end{array}\right\} \Rightarrow MCD(36,28) = r_2 = 4$$

ESEMPIO 2 $\quad MCD(2420, 1386) = \dots$

1° PASSAGGIO

$$\underbrace{2420}_{a} = \underbrace{1386}_{b} \cdot \underbrace{1}_{q_1} + \underbrace{1034}_{r_1}$$

2° PASSAGGIO

$$\underbrace{1386}_{b} = \underbrace{1034}_{r_1} \cdot \underbrace{1}_{q_2} + \underbrace{352}_{r_2}$$

3° PASSAGGIO

$$\underbrace{1034}_{r_1} = \underbrace{352}_{r_2} \cdot \underbrace{2}_{q_3} + \underbrace{330}_{r_3}$$

4° PASSAGGIO

$$\overbrace{352}^{r_2} = \overbrace{330}^{r_3} \cdot \overbrace{1}^{q_4} + \overbrace{22}^{r_4}$$

5° PASSAGGIO

$$\underbrace{330}_{r_3} = \underbrace{22}_{r_4} \cdot \underbrace{15}_{q_5} + \underbrace{0}_{r_5}$$

$$\left.\begin{array}{l} r_5 = 0 \\ r_4 \neq 0 \end{array}\right\} \Rightarrow MCD(2420, 1386) = r_4 = 22$$

CALCOLO DI MCD IN $\mathbb{Z}$

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Per calcolare $MCD(a,b)$ si può procedere in uno dei due seguenti modi:

1° MODO

- calcolare $|a|, |b| \in \mathbb{N}$
- calcolare $MCD(|a|, |b|) = d \in \mathbb{N}$
- osservare che allora d e $-d$ sono i due $MCD(a,b)$ in $\mathbb{Z}$

2° MODO

- usare l'algoritmo di Euclide in $\mathbb{Z}$: si eseguono divisioni successive in $\mathbb{Z}$

(ATTENZIONE: tutti i resti devono essere non negativi!)

e l'ultimo resto non nullo nella sequenza di queste divisioni è il massimo comun divisore positivo d'a e b in $\mathbb{Z}$

ESEMPIO Calcoliamo $MCD(-274, 110)$ in due modi

1° MODO $\quad a = -274$, $b = 110$ per cui $|a| = 274$, $|b| = 110$

$$\underbrace{274}_{|a|} = \underbrace{110}_{|b|} \cdot \underbrace{2}_{q_1} + \underbrace{54}_{r_1}$$

$$\underbrace{110}_{|b|} = \underbrace{54}_{r_1} \cdot \underbrace{2}_{q_2} + \underbrace{2}_{r_2}$$

$$\underbrace{54}_{r_1} = \underbrace{2}_{r_2} \cdot \underbrace{27}_{q_3} + \underbrace{0}_{r_3} \Rightarrow$$

$MCD(|a|, |b|) = 2$ per cui 2 e -2 sono i due massimi comun divisori di $a = -274$ e $b = 110$ in $\mathbb{Z}$

2° MODO

$a = -274$
$b = 110$

$$\overbrace{-274}^{a} = \overbrace{110}^{b}\cdot\overbrace{(-3)}^{q_1}+\overbrace{56}^{r_1}$$

$$\overbrace{110}^{b} = \overbrace{56}^{r_1}\cdot\overbrace{1}^{q_2}+\overbrace{54}^{r_2}$$

$$\overbrace{56}^{r_1} = \overbrace{54}^{r_2}\cdot\underbrace{1}_{q_3}+\underbrace{2}_{r_3}$$

$$\underbrace{54}_{r_2} = \underbrace{2}_{r_3}\cdot\underbrace{27}_{q_4}+\underbrace{0}_{r_4}$$

$\Rightarrow$ $r_3 = 2 = MCD(a,b)$ e 2 e -2 sono i due massimi comuni divisori di $a=-274$ e $b=110$ in $\mathbb{Z}$

PER CASA: ESERCIZIO 2 (file: I19casaT1.pdf)