Lezione 18-10

martedì 18 ottobre 2022 11:09

## CONSEGUENZE del TEOREMA di BEZOUT

① $\forall a,b,c \in \mathbb{Z}$, se $a \mid bc$ e $MCD(a,b)=1 \Rightarrow a \mid c$

Dim

Per ipotesi $MCD(a,b)=1 \Rightarrow \exists u,v \in \mathbb{Z}$ t.c. $1 = ua + vb$ .

Moltiplico per $c$ e ottengo $c = uac + vbc$ . Per ipotesi $a \mid bc$

e quindi esiste $k \in \mathbb{Z}$ t.c $bc = a \cdot k$ . Sostituisco e ottengo

$c = uac + vak = a(uc + vk) \Rightarrow c$ è multiplo di $a$ e cioè $a \mid c$ □

② $\forall a,b \in \mathbb{Z}$, $p$ numero primo in $\mathbb{Z}$ . Se $p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$ .

Dim per casa

DEF - Dati $a,b \in \mathbb{Z}$, $m$ è detto MINIMO COMUNE MULTIPLO di $a$ e $b$ se:

(1) $a \mid m$ e $b \mid m$ ($m$ è multiplo sia di $a$ che di $b$) $a,b \in D(m)$

(2) $\forall t \in \mathbb{Z}$ tale che $a \mid t$ e $b \mid t \Rightarrow m \mid t$ .

### PROPOSIZIONE

Dati $a,b \in \mathbb{Z}$, $d = MCD(a,b)$ e siano $a'$ e $b'$ tali che $a = a'd$ e $b = b'd$ $MCD(a',b') = 1$ . Si ha:

1) $m := a'b'd$ è un minimo comune multiplo per $a$ e $b$

2) $m'$ è m.c.m. per $a$ e $b \Leftrightarrow m' = \pm m$

Dim

1) Vediamo che $m := a'b'd$ soddisfa le 2 condizioni della definizione di mcm.

Per la ①, si ha $m = a'b'd = (a'd)b' = ab' \Rightarrow m$ è multiplo di $a$

$m = a'b'd = a'(b'd) = a'b \Rightarrow m$ è multiplo di $b$

Per la ②, sia $t$ tale che $a \mid t$ e $b \mid t$ . Per definizione di $|$, esistono

$h,k \in \mathbb{Z}$ tali che $t = ha$ e $t = kb \Rightarrow t = ha'd = kb'd$

Quindi $ha' = kb'$, (semplificando $d$)

Quindi $ha' = kb'$ (semplificando d)

$b'$ divide $ha' \Rightarrow b' \mid ha'$ e per ipotesi $MCD(a', b') = 1$

$\Rightarrow$ per la I conseguenza del th di Bezout, $b' \mid h$, cioè $\exists\, l$ t.c $h = b'l$

Di conseguenza, $t = b'l\,a'd = (a'b'd)l = ml \Rightarrow m \mid t$ CVD

② è uguale alla dimostrazione per MCD $\square$

NOTAZIONE: $mcm(a,b)$ sarà il positivo tra $m$ e $-m$

OSSERVAZIONE: $mcm(a,b) = a'b' MCD(a,b)$

$mcm(a,b)\, MCD(a,b) = a'b' MCD(a,b)\, MCD(a,b)$

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

$a \qquad b$

$$|ab| = mcm(a,b)\, MCD(a,b)$$

$$mcm(a,b) = \frac{|ab|}{MCD(a,b)}$$

ESEMPIO: $mcm(494, 214)$

Devo prima trovare $MCD(494, 214)$

$494 = 214 \cdot 2 + 66$ $\rightarrow$ $66 = 494 - 2 \cdot 214 = 494 + (-2) \cdot 214$

$214 = 66 \cdot 3 + 16$ $\rightarrow$ $16 = 214 - 3 \cdot 66$

$66 = 16 \cdot 4 + 2$ $\rightarrow$ $2 = 66 - 16 \cdot 4$

$16 = 2 \cdot 8 + 0$

$MCD(494, 214) = 2 \Rightarrow mcm(494, 214) = \frac{214 \cdot 494}{2} = 52858$

$2 = u \cdot 214 + v \cdot 494$ ?

$$2 = 66 + (-4)\cdot 16 = 66 + (-4)(214 + (-3)\cdot 66) = \underline{66} + (-4)214 + (12)\cdot\underline{66}$$

$$= 13\cdot 66 + (-4)\,214 =$$

$$= 13\cdot(494 + (-2)\cdot 214) + (-4)\,214 =$$

$$= 13\cdot 494 + (-26)\cdot 214 + (-4)\,214 =$$

$$= \underbrace{13}_{u=13}\cdot 494 + \underbrace{(-30)}_{v=-30}\cdot 214$$

**DEF** - Sia $m\mathbb{Z} \subseteq \mathbb{Z}\times\mathbb{Z}$ la relazione definita da:

$a \; m\mathbb{Z} \; b \iff$ $a-b$ è multiplo di $m$

$\exists k \in \mathbb{Z}$ t.c. $a-b = mk$

$\exists k \in \mathbb{Z}$ t.c. $a = b+mk$

$m \mid (a-b)$

} equivalenti

$m\mathbb{Z}$ si chiama CONGRUENZA MODULO $m$

**TEOREMA**

$m\mathbb{Z}$ è una RELAZIONE di equivalenza compatibile con $+$ e $\cdot$, cioè

se $a \; m\mathbb{Z} \; b$ e $c \; m\mathbb{Z} \; d \implies a+c \; m\mathbb{Z} \; b+d$ e $ac \; m\mathbb{Z} \; bd$

**Dim**

Vediamo che $m\mathbb{Z}$ è R.e.

(i) Riflessiva: $\forall a \in \mathbb{Z}$, $a \; m\mathbb{Z} \; a$ ?

Vero perché $a-a = 0 = 0\cdot m \implies m \mid 0$

(ii) Simmetrica: $\forall a,b \in \mathbb{Z}$ se $a \; m\mathbb{Z} \; b \implies b \; m\mathbb{Z} \; a$ ?

Se $a \; m\mathbb{Z} \; b$ allora $\exists k \in \mathbb{Z}$ tc $a-b = mk$.

Quindi $b-a = (-k)\,m$ (moltiplicando per $-1$)

$\implies m \mid b-a$ e $b \; m\mathbb{Z} \; a$

(iii) Transitiva: $\forall a,b,c \in \mathbb{Z}$ si $(a \; m\mathbb{Z} \; b \text{ e } b \; m\mathbb{Z} \; c) \Rightarrow a \; m\mathbb{Z} \; c$ ?

Per ipotesi $\exists k,h \in \mathbb{Z}$ t.c. $a-b = mh$ e $b-c = mk$ $\quad$ $\exists \ell$ t.c. $a-c = m\ell$

$b = c + mk$

$\Rightarrow$ sostituisco ed ho $a-(c+mk) = mh$

$a - c - mk = mh \quad \Rightarrow \quad a-c = mk + mh$

$\Rightarrow \quad a-c = m(k+h)$ ✓

(2) Vediamo che si $a \; m\mathbb{Z} \; b$ e $c \; m\mathbb{Z} \; d \Rightarrow$ $a+c \; m\mathbb{Z} \; b+d$, $ac \; m\mathbb{Z} \; bd$

Per ipotesi $\exists h,k \in \mathbb{Z}$ tali che $a-b = mh$ e $c-d = mk$

Tesi: $\exists \ell, s$ tali che $(a+c)-(b+d) = \ell m$ e $ac - bd = sm$

Dalle ipotesi ho $(a-b)+(c-d) = mh + mk$

$a - b + c - d = (a+c) - (b+d)$

allora $(a+c) - (b+d) = m(h+k) \Rightarrow (a+c) \; m\mathbb{Z} \; (b+d)$

Dalle ipotesi, moltiplicando per $c$ ho $(a-b)c = mhc$

moltiplicando per $b$ ho $(c-d)b = mkb$

sommo membro a membro e ricavo $(a-b)c + (c-d)b = m(hc+kb)$

$= ac - bc + cb - db$

$= ac - db$

$\Rightarrow \quad ac - db = m(hc+kb) \Rightarrow ac \; m\mathbb{Z} \; db$

□

ESEMPIO

$a \; 3\mathbb{Z} \; b \iff a-b = 3k \iff a = b + 3k$

$a=1 \rightarrow b=4 \qquad 1 \; (3\mathbb{Z}) \; 4 \qquad 1-4 = 3(-1)$

$2 \; 4\mathbb{Z} \; 6$

$2 \; 4\mathbb{Z} \; 10$

2 e 6 hanno lo stesso resto nella divisione per 4

$2 = 4 \cdot 0 + 2$

$2 \; 4\mathbb{Z} \; 10$ $\Big\}$ 2 e 6 hanno lo stesso resto nella divisione per 4

$2 = 4 \cdot 0 + 2$

$6 = 4 \cdot 1 + 2$

$10 = 4 \cdot 2 + 2$

$-1 \; 5\mathbb{Z} \; 4$

$-1 \; 5\mathbb{Z} \; 9$

NOTAZIONE $\quad a \; m\mathbb{Z} \; b \qquad a \equiv_m b \qquad a \equiv b \pmod m$

DEF - L'insieme quoziente $\mathbb{Z}/m\mathbb{Z}$ verrà denotato con $\mathbb{Z}_m$ e chiamato insieme degli interi modulo m.

Gli elementi di $\mathbb{Z}_m$ li denotiamo con $[x]_m$ oppure $\bar{x}$ _

OSSERVAZIONI

1) Dato $m \in \mathbb{Z}$ e $x \in \mathbb{Z}$, $[x]_m = \{x + mk \mid k \in \mathbb{Z}\}$

$[1]_4 = \{1 + 4k \mid k \in \mathbb{Z}\} = \{\dots -7, -3, 1, 5, 9, \dots\}$

2) $\forall x \in \mathbb{Z}$, $x$ $m \neq 0$ $\quad [x]_m = [\text{rest}(x, m)]_m$

$\Downarrow$

$x = mq + r$ e $x - r = mq \Rightarrow x \equiv_m \text{rest}(x, m)$

3) $\forall x \in \mathbb{Z}$, $[x]_0 = \{x\}$ (perché $x + mk = x$ se $m = 0$)

4) Se $m \neq 0$ $[x]_m$ è infinita

5) Se $m > 0$ e $0 < a, b < m$, $a \equiv_m b \iff a = b$

"$\Leftarrow$" (Dim) Se $a = b \Rightarrow a$ è in relazione con $b$ per la proprietà riflessiva di $m\mathbb{Z}$

"$\Rightarrow$" Se $a \equiv_m b$, allora $a = b + mk$ con $k \geq 0$ (supponiamo che $a \geq b$)

$a - b \leq a < m \Rightarrow k \leq 0$. Quindi $k = 0$ e $a = b$ □

TEOREMA

Sia $m > 0$, $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$ _ Quindi $|\mathbb{Z}_m| = m$

Dim

$\forall x \in \mathbb{Z}$, $[x]_m = [\text{rest}(x,m)]_m$ e $0 \le \text{rest}(x,m) \le m-1$ e dal punto ⑤ dell'osservazione, a resti diversi corrispondono classi diverse □

Es- $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

**LEMMA** sul

Dati $a, b, m \in \mathbb{Z}$,

① $a \equiv b \pmod m \iff \forall t \in \mathbb{Z} \quad a+t \equiv b+t \pmod m$

② $a \equiv b \pmod m \implies \forall t \in \mathbb{Z} \quad at \equiv bt \pmod m$

③ $\&$ $at \equiv bt \pmod m$ e $MCD(m,t) = 1 \implies a \equiv b \pmod m$

Es- $1 \equiv 4 \pmod 3 \rightarrow 1+5 \equiv 4+5 \pmod 3$

$\rightarrow 1-4 \equiv 4-4 \pmod 3$

$\rightarrow 1 \cdot 2 \equiv 4 \cdot 2 \mod 3$
$1 \cdot 6 \equiv 4 \cdot 6 \mod 3$

$12 \equiv 0 \pmod 6$

$3 \cdot 4 \equiv 0 \cdot 4 \pmod 6$ No! $MCD(4,6) \neq 1$

$3 \not\equiv 0 \pmod 6$