

Tutorato

Elisa Scandivuzzi

email: scandivuzzi.2069644

@studenti.uniroma1.it

Inizio: Probabilmente
prossima settimana,
controllare gruppo.

Esercitazione: Stessa stanza Gmeet

17 - 18:30

Aritmetica: Struttura degli interi

Parole chiave:

- * Divisione con resto
- * Massimo comun divisore.

Identità di Bezout

Algoritmo Euclideo

- * Equazioni Diotantine
-

Divisione con resto

Proposizione: Dati $a, b \in \mathbb{Z} - \{0\}$
Esistono unici $q, r \in \mathbb{Z}$
(quoziente e resto)

t.c.

$$a = b \cdot q + r$$

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

Dim. Dobbiamo mostrare l'esistenza
e l'unicità

Esistenza

Oss: possiamo ricondursi sempre
al caso in cui $a, b > 0$

① Se $a < 0$ e $b > 0$

$$\downarrow$$

$$-a > 0$$

siccome $-a, b > 0$ e stiamo
assumendo di saper risolvere
il caso "positivo"

$$-a = b \cdot q + r \in |r| < |b|$$

$$\Rightarrow a = \underbrace{-q \cdot b}_{\downarrow} + \underbrace{r}_{\downarrow}$$

② se $a > 0$ e $b < 0$

$$\begin{matrix} \downarrow \\ -b > 0 \end{matrix}$$

caso positivo $\Rightarrow a = q(-b) + r$ cons

$$|r| < |b| \\ || \\ |b|$$

$$\Rightarrow a = -qb + r$$

③ $a < 0 \quad e \quad b < 0$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ -a > 0 & & -b > 0 \end{array}$$

caso positivo $\Rightarrow -a = q(-b) + r \quad |r| < |b|$

$$|| \\ |b|$$

$$\Rightarrow a = bq - r = bq + r'$$

$$r' = -r$$

$$|r'| = |r| < |b|$$

\Rightarrow E' suff. mostrare l'esistenza
di q e r quando $a, b > 0$.

Consideriamo

$$S = \{q \in \mathbb{N} \mid b(q+1) > a\}$$

$$S \subset \mathbb{N}$$

$S \neq \emptyset$ perche' contiene
almeno $a \in S$

$$b(a+1) = ba + a > a$$

\Rightarrow Siccome \mathbb{N} e' ben ordinato

S ammette un minimo

$$q = \min(S)$$

Quali proprietà?

$$q \in S \Rightarrow b(q+1) > a$$

q e' il minimo per cui $b(q+1) > a$
necessariamente $a \geq bq$

altrimenti $q-1 < q$ apparterebbe
a S contraddicendo la minimalità

$$bq \leq a < b(q+1)$$

$$\Rightarrow a = bq + r$$

$$\text{e } r < b(q+1) - bq = b \quad \not\propto$$

Unicità: Supponiamo che

$$a = bq + r \quad 0 \leq r < |b|$$

ma anche

$$a = bq' + r' \quad 0 \leq r' < |b|$$

\Rightarrow vogliamo dedurre che $q = q'$
 $r = r'$

$$\underline{bq + r = bq' + r'}$$

$$\Rightarrow b(q - q') = r' - r$$

$$\Rightarrow |b| \cdot |q - q'| = |r' - r|$$

$|q - q'|$ è
differenza tra
due numeri $0 \leq r, r' < |b|$

è sempre $< |b|$

è sempre $< |b|$

di b , in

particolare se

non è zero

e necessariamente

$$\geq |b|$$

$\geq |b|$

L'unica possibilità è che $|q-q'|=0$
 $\Rightarrow q=q'$
 $\Rightarrow r=r'$



Caso particolare $r=0$

In questo caso $a=b \cdot q$

Def(Divisibilità) Diciamo che b divide a (e scriviamo $b|a$)
se $a=bq$ per qualche $q \in \mathbb{Z}$.

Negli esercizi: la divisibilità è
una relazione d'ordine parziale
su \mathbb{N} .

Oss 1} Se $b|a$ e $b|c$
allora $b|x+cy$ $\forall x, y \in \mathbb{Z}$

Dim. $b \mid a \Leftrightarrow \frac{a}{b} = q$
 $b \mid c \Leftrightarrow \frac{c}{b} = t$

$$\begin{aligned} ax + cy &= bqx + bty \\ &= b(qx + ty) \end{aligned}$$

Fissiamo ora una coppia $a, b \in \mathbb{Z}$
possiamo considerare l'insieme
dei divisori comuni (positivi)

$$D = \{ d \in \mathbb{N} \mid d \mid a \text{ e } d \mid b \}$$

Def (Massimo Comun Divisore)

Chiamiamo massimo comun divisore
di a e b ($\in \mathbb{Z}$) il massimo
elemento di D 
con $\text{mcd}(a, b)$
rispetto alla relazione
di divisibilità

$$\begin{array}{l}
 \left\{ \begin{array}{l}
 \textcircled{1} \quad \text{mcd}(a,b) \mid a \text{ e } \text{mcd}(a,b) \mid b \\
 \textcircled{2} \quad \text{se } d \mid a \text{ e } d \mid b \\
 \end{array} \right. \\
 \hline
 \Rightarrow d \mid \text{mcd}(a,b)
 \end{array}$$

Teorema: Dati $a, b \in \mathbb{Z}_{\neq 0}$ esiste
 sempre il massimo comun divisore
 $\text{mcd}(a,b) \in \mathbb{N}$. Inoltre vale
 sempre la seguente identità
 di Bezout: $\exists x, y \in \mathbb{Z}$ t.c.

$$\boxed{\text{mcd}(a,b) = ax + by.}$$

Dim. Consideriamo l'insieme

$$\begin{aligned}
 S &= \left\{ d \in \mathbb{N}_{\geq 0} \mid d = ax + by \right\} \\
 &= \text{per qualche } x, y \in \mathbb{Z} \\
 &= \left\{ ax + by > 0 \right\}_{x, y \in \mathbb{Z}}
 \end{aligned}$$

Oss: $S \neq \emptyset$ se $a > 0$
 troviamo $a \cdot 1 + b \in S$
 a''
 se $a < 0$
 troviamo $-1 \cdot a + b \in S$
 a''

Per il principio del minimo
 esiste il minimo elemento
 di S $\underline{d = ax + by}$.

Claim: \underline{d} è il massimo
 comune divisore fra a e b

Dim. Mostriamo che se $k | a$ e
 $k | b$ allora $k | d$

Questo segue semplicemente
 dall'osservazione fatta prima
 (vedere Oss 1)

Resta da vedere che $d \mid a$ ed b

Supponiamo non sia così

caso $d \nmid a$

\Rightarrow facciamo la divisione
con resto:

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

Siccome $d \nmid a$ necessariamente
 $r \neq 0$

Dunque abbiamo che

$0 < r < d$ soddisfa

$$r = a - dq$$

$$= a - (ax + by)q$$



$$= a(1 - qx) + b qy$$

$$d = ax + by$$

\Rightarrow anche r è un elemento di S
 però avevamo scelto d come
 $\min(S)$ e $r < d$ questo
 porta alla contraddizione desiderata.
 \Rightarrow Necessariamente $d \mid a$.

Allo stesso modo concludiamo che $d \mid b$
 $\Rightarrow d = \text{mcd}(a, b) \neq$

Lemma: Dati $a, b \in \mathbb{Z}$ vale sempre

$$\text{mcd}(a, b) = \text{mcd}(a + kb, b)$$

$$\forall k \in \mathbb{Z}.$$

Applicazione: $\text{mcd}(\underline{305}, \underline{298})$

$\left[\begin{array}{l} \text{ "Lemma} \\ \text{mcd}(305 - 298, 298) \\ \text{ " } \\ \text{mcd}(\underline{7}, \underline{298}) \end{array} \right]$

Questo
 procedimento
 che consiste
 nell'applicare
 il Lemma
 molte volte
 e' quello
 che si chiama
 algoritmo Euclideo
 per il MCD.

$$\begin{aligned}
 & \text{Il Lemma} \\
 & \text{mcd}(7, 18) = 298 - 7 \cdot 40 \\
 & \quad \parallel \\
 & \text{mcd}(7, 18) \\
 & \quad \parallel \text{Lemma} \\
 & \text{mcd}(7, 18 - 7 \cdot 2) \\
 & \quad (7, 4) \\
 & \quad \parallel \\
 & \quad \vdots = 1
 \end{aligned}$$

poco
 efficiente,
 avrei potuto
 - 294.

Dim. Dobbiamo dim. che
 $\text{mcd}(a + kb, b) = \text{mcd}(a, b)$

mostriamo che $D = \text{mcd}(a + kb, b)$
 ha le proprietà di $\text{mcd}(a, b)$

$$① D | a \wedge D | b$$

$$② \text{ se } t | a \wedge t | b \Rightarrow k | D$$

$$\text{Dim ② } t \mid a \Rightarrow t \mid a + kb \Rightarrow t \mid b$$

$$\text{Dim} \textcircled{1} \quad D = \text{mod}(a + kb, b) \mid a$$

Sappiamo che

$$D \mid a+kb$$

D | b \implies D {b gratis}

$$D \mid (a + kb) - kb = a$$

Questo termina la dim. 

Algoritmo Euclideo per il MCD

$a, b \in \mathbb{N}$ e supponiamo $a \geq b$

Step 1: Divisione con resto

$$a = bq_0 + r_0 \rightarrow \text{mcd}(a, b) \underset{\text{II Lemma}}{=} \text{mcd}(b, a - bq_0)$$

Step 2: Ripartiamo da b e r_0 $\parallel r_0 < b$

$$b = q_1 r_0 + r_1 \quad \text{mcd}(b - q_1 r_0, r_0) \underset{\text{II Lemma}}{=} r_1$$

: procediamo allo stesso modo

:

Osserviamo che a un certo punto
dobbiamo necessariamente fermarci
perche' la successione dei resti

$$r_0 > r_1 > r_2 > \dots$$

e' strettamente decrescente

(infatti r_n sara' il resto della divisione di r_{n-2} per r_{n-1})

\Rightarrow A un certo punto

otteniamo $r_N = 0$ cioè

$$r_{N-2} = q r_{N-1} \quad \text{ovvero } r_{N-1} \mid r_{N-2}$$

Ora, riguardiamo la successione degli MCD: Abbiamo

$$\text{mcd}(a, b)$$

"

$$\text{mcd}(a - bq_0, b) = \text{mcd}(r_0, b)$$

$$= \text{mcd}(r_0, b - q_1 r_0)$$

$$= \text{mcd}(r_0, r_1)$$

$$= \text{mcd}(r_1, r_2)$$

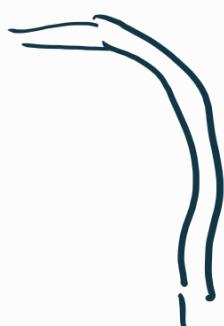
$$= \dots$$

$$= \text{mcd}(r_{N-2}, r_{N-1})$$

$\overrightarrow{r} = r_{N-1} \neq$
 Siccome $r_{N-1} \mid r_{N-2}$

Esempio:

$\text{MCD}(462, 244)$



$$\begin{array}{cccc}
 a & b & q_0 & r_0 \\
 \parallel & \parallel & \parallel & \parallel \\
 462 & = 244 \cdot 1 + 218 & & \\
 & & & \text{mod}(244, 218) \\
 b & & r_0 & q_1 & r_1 \\
 \parallel & & \parallel & \parallel & \parallel \\
 244 & = 218 \cdot 1 + 26 & & & \parallel \\
 & & & & (218, 26) \\
 r_0 & & r_1 & q_2 & r_2 \\
 \parallel & & \parallel & \parallel & \parallel \\
 218 & = 26 \cdot 8 + 10 & & & \parallel \\
 & & & & (26, 10) = 2
 \end{array}$$

$$\begin{array}{cccc}
 r_1 & r_2 & q_3 & r_3 \\
 \parallel & \parallel & \parallel & \parallel \\
 26 & = 10 \cdot 2 + 6 & &
 \end{array}$$

$$\begin{array}{cccc}
 r_2 & r_3 & q_4 & r_4 \\
 \parallel & \parallel & \parallel & \parallel \\
 10 & = 6 \cdot 1 + 4 & &
 \end{array}$$

$$\begin{array}{cccc}
 r_3 & r_4 & q_5 & r_5 \\
 \parallel & \parallel & \parallel & \parallel \\
 6 & = 4 \cdot 1 + 2 & &
 \end{array}$$

$$4 = 2 \cdot \textcircled{2} \longrightarrow \text{MCD}!$$

Equazioni Diofantee

$$ax + by = c \quad \text{con } a, b, c \in \mathbb{Z}$$

(Come) si risolvono? (In \mathbb{Z} , cioè esistono $x, y \in \mathbb{Z}$ che risolvono),
Quante soluzioni? Possiamo descriverle tutte?

Esempio 1: $x + y = 0$ Ha sol? SI

$$x = -y$$

$$x + y = 1 \quad \text{Ha sol? SI}$$

$$x = 1 - y$$

$$\underbrace{2x + 4y = 3}_{\text{pari}} \quad \text{Ha sol? NO}$$

↑ dispari

$$\underbrace{15x + 20y = 7}_{\text{il lato sx e' multiplo di 5, il dx no.}} \quad \text{Ha sol? NO}$$

In generale, se $\text{mcd}(a,b) \nmid c$

l'eq. $ax+by=c$ non ha soluzioni

questo è sempre
un multiplo di $\text{mcd}(a,b)$

Teorema: Se $\text{mcd}(a,b) \mid c$ allora
 $ax+by=c$ ammette soluzione.

Dim. Sappiamo per l'identità di Bezout
che esistono $x_0, y_0 \in \mathbb{Z}$ t.c.

$$ax_0 + by_0 = \text{mcd}(a,b) = D$$

siccome $D \mid c$ abbiamo anche

$$c = Dk$$

$$\Rightarrow (ax_0 + by_0)k = Dk = c$$

$$\Rightarrow \begin{cases} X = X_0 \cdot k \\ Y = Y_0 \cdot k \end{cases} \text{ risolvono l'eq.}$$

Questa \uparrow che abbiamo trovato
e' una soluzione, ne esistono
altre? SI.

Supponiamo di avere una
soluzione (x_1, y_1) di
 $ax + by = c$

Allora anche $(x_1 + tb, y_1 - ta)$
e' una soluzione! ($\forall t \in \mathbb{Z}$)

$$a(x_1 + tb) + b(y_1 - ta) =$$

$$= (ax_1 + by_1) + tab - tab$$

$$= ax_1 + by_1 = c$$

\Rightarrow Se esiste una soluzione
ne esistono infinite.

Come le troviamo tutte?

Oss: Supponiamo che (x_1, y_1)
e (x_2, y_2) siano soluzioni

$$ax_1 + by_1 = c = ax_2 + by_2$$

$$\Rightarrow a(x_1 - x_2) + b(y_1 - y_2) = 0$$

$\Rightarrow (x_1 - x_2, y_1 - y_2)$ è una
soluzione di $ax + by = 0$

(stessa equazione senza termine
noto). Ne deduciamo che
le soluzioni hanno la forma

$$(x_1, y_1) \text{ soluzione di } ax + by = c$$

+

(x_0, y_0) soluzione di $\boxed{ax+by=0}$

\downarrow

Prop. Le soluzioni di $ax+by=0$
sono tutte della forma

$$x = k \frac{b}{\text{mcd}(a,b)} \quad y = -k \frac{a}{\text{mcd}(a,b)}$$

Esempio: ① $2x+7y=0$
 $\rightarrow (+7k, -2k) \quad k \in \mathbb{Z}$

② $9x+12y=0$



$$3x+4y=0$$

$$\neq (4k, -3k)$$

$$l_1 = \frac{12}{\text{mcd}(9, 12)}$$

$$3 = \frac{9}{\text{mcd}(9, 12)}$$

In conclusione:

Teorema: Consideriamo

$$ax + by = c$$

① $\text{mcd}(a, b) \nmid c \Rightarrow$ no sol.

② $\text{mcd}(a, b) \mid c \Rightarrow$ le sol.

Sono tutte e sole quelle
della forma

$$\begin{cases} x = x_0 + \frac{b}{\text{mcd}(a, b)} k \\ y = y_0 - \frac{a}{\text{mcd}(a, b)} k \end{cases} \quad k \in \mathbb{Z}$$

(x_0, y_0) è una qualsiasi

$$\text{sol. di } \underbrace{ax+by=c}_{\uparrow}$$

Questa sol particolare
si trova con l'algoritmo
Euclideo (identità
di Bezout).

Esempio:

$$4x + 5y = 7$$

Step 1: Trovare sol. particolare

$$x = 3 \quad y = -1$$

$$4 \cdot 3 - 5 \cdot 1 = 12 - 5 = 7$$

$$\begin{cases} x_0 = 3 \\ y_0 = -1 \end{cases}$$

Step 2: Trovare tutte le sol

$$4x + 5y = 0 \iff 4x = -5y$$

$$x = 5k$$

$$y = -4k$$

mult 4

$$4x \Rightarrow y = 4k$$

$$\Rightarrow 4x = -5 \cdot 4k$$

$$\Rightarrow x = -5k$$

Step 3 mettere assieme

$$4x + 5y = 7$$

$$(x_0 + 5k, y_0 - 4k) = (3 + 5k, -1 - 4k)$$

$$(3 + 10, -1 - 8) = (13, -9)$$

$$(3 - 5, -1 + 4) = (-2, 3)$$

Esempio:

$$38x + 58y = 101$$

$\underbrace{}$ \nwarrow dispari
pari

$$25x + 17y = 21$$

Step 1: Sol partolare

Algoritmo:

$$\begin{array}{r} 25 = 17 \cdot 1 + 8 \\ 17 = 8 \cdot 2 + 1 \\ \hline 8 = 8 \cdot 1 + 0 \end{array}$$

\Downarrow

$$\begin{aligned} 21 \cdot 1 &= 17 - 8 \cdot 2 & 8 &= 25 - 17 \cdot 1 \\ &= 17 - (25 - 17) \cdot 2 & & \\ &= (17 \cdot 3 - 25 \cdot 2) \cdot 21 & & \end{aligned}$$

MCD

Per trovare una sol. particolare
di $25x + 17y = 21$, basta moltiplicare per 21

$$21 = 17 \cdot 63 - 25 \cdot 42$$

$$x_0 = 63$$

$$y_0 = -42$$

Step 2: Trovare tutte le sol. di

$$25x + 17y = 0$$

$$\begin{aligned} & \boxed{25x = -17y} \\ & \boxed{25 \nmid 17 \Rightarrow 25 \mid y} \\ & \Rightarrow y = 25k \end{aligned}$$

$$\Rightarrow x = -17k$$

Step 3: Tutte le sol. di

$$25x + 17y = 21$$

$$\begin{cases} x = 63 - 17k \\ y = -42 + 25k \end{cases}$$

Def (Coprimenti) Diciamo che

$a, b \in \mathbb{Z}$ sono coprimenti

se $\text{mcd}(a, b) = 1$

Lemma: Se $\text{mcd}(a, c) = 1$ e
 $a | bc$ allora $a | b$

Come applicazione: $25 | 17x \Rightarrow 25 | x$
 $1 = \text{mcd}(25, 17)$

Dim. Per Bezout $\text{mcd}(a, b) = s$

$$\Rightarrow ax + cy = 1 \text{ per qualche}$$

$$x, y \in \mathbb{Z} \quad \downarrow \cdot b$$

$$\Rightarrow b(ax + cy) = b$$

||

$$\underbrace{abx}_{a|} + \underbrace{bcy}_{a|} = b$$

Sappiamo che $a | bc$

$$a | bc \Rightarrow a | \underbrace{abx}_{a|} + \underbrace{bcy}_{a|} = b$$

✓

Riassunto:

① Divisione con resto

$$a = bq + r \quad 0 \leq r < |b|$$

② MCD: Esistenza

Identità di Bezout

$$\text{mcd}(a, b) = ax + by$$

$$\textcircled{3} \quad \text{mcd}(a+kb, b) = \text{mcd}(a, b)$$



Algoritmo Euclideo delle divisioni successive (ultimo resto ≠ 0 è il MCD)



Invertendo i passaggi dell'ALG otteniamo anche gli x e y che compaiono in Bezout.

④ Equazioni Diophantee

$$ax + by = c \quad a, b, c \in \mathbb{Z}$$

Risolvibilità $\Leftrightarrow \text{mcd}(a, b) | c$

Descritto tutte le soluzioni:

Sol particolare (x_0, y_0) tramite ALG Euclideo (invertito)

Tutte le sol di $ax+by=0$

Combinando le due otteniamo
tutte le sol. dell'eq. di partenza

⑤ Coprimi: Caso in cui $\text{mcd}(a,b)=1$,
permette di semplificare
le rel. di div.

$$ax+by=c \rightarrow \begin{aligned} & \text{mcd}(a,a)=a \\ & \text{Risolvibilità} \Leftrightarrow a|c \\ & \text{Se } a|c \quad c = aq \\ & \text{allora } ax+ay=c \\ & \text{e' equiv. a} \\ & x+y=q \\ & \Leftrightarrow x = q-y \end{aligned}$$

⚠ $a, b \neq 0$!

