

L' "anello" dei numeri interi:

(1)

OPERAZIONI

DIVISIBILITÀ

FATTORIZZAZIONE

L'insieme degli interi può essere identificato così:

$$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$$

In esso sono definite due operazioni binarie interne

$+$: somma \cdot : prodotto

per cui valgono le ben note regole di calcolo:

- $\forall z_1, z_2 \in \mathbb{Z}$: $\underline{z_1 + z_2 \in \mathbb{Z}}$ e $\underline{z_1 \cdot z_2 \in \mathbb{Z}}$
- $\forall z_1, z_2 \in \mathbb{Z}$: $z_1 + z_2 = z_2 + z_1$ e $z_1 \cdot z_2 = z_2 \cdot z_1$
(proprietà commutative)
- $\forall z_1, z_2, z_3 \in \mathbb{Z}$ $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ e
 $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 + z_3)$
(proprietà associative)
- \exists un elem. $\in \mathbb{Z}$ (zero: 0) tale che
 $\forall z \in \mathbb{Z}$ si abbia $z + 0 = z$ { esistenza
- \exists un elem. $\in \mathbb{Z}$ (unità: 1) tale che { dei neutrî
 $\forall z \in \mathbb{Z}$ si abbia $z \cdot 1 = z$
- $\forall z \in \mathbb{Z}$ esiste in \mathbb{Z} un elem. (opposto di z : $-z$)
tale che $z + (-z) = 0$
- $\forall z_1, z_2, z_3$: $(z_1 + z_2) \cdot z_3 = z_1 z_3 + z_2 z_3$ (distributività)

(2)

A partire da queste operazioni e loro proprietà si riesce a definire anche un'altra operazione binaria interna: la differenza

$$\forall z_1, z_2 \in \mathbb{Z} : z_1 - z_2 = z_1 + (-z_2) \in \mathbb{Z}$$

(per la quale non valgono la prop. comm.
e associativa:

$$5 - 3 = 2$$

$$3 - 5 = -2$$

$$3 - (2 - 4) = 3 - (-2) = 5 \quad (3 - 2) - 4 = 1 - 4 = -3$$

mentre vale la proprietà distributiva:

$$\forall z_1, z_2, z_3 \in \mathbb{Z} : (z_1 - z_2) \cdot z_3 = z_1 z_3 - z_2 z_3$$

Siamo abituati ad associare alla "differenza" l'idea di "operazione inversa della somma" e similmente a pensare la "divisione" come "operazione inversa del prodotto".

Ma ciò non è sempre possibile in \mathbb{Z} , poiché non ogni intero a si può ottenere da un altro intero b moltiplicando quest'ultimo per un opportuno intero q.

ad es. $a = 5$, $b = 2$: $5 = 2q$
non ha soluzioni intere.

Serve precisare.

OSSERVAZIONE: $\forall q \in \mathbb{Z}$ si ha $0 \cdot q = 0$.

Quindi nei problemi di divisibilità non ha senso prendere il divisore $b = 0$.

Divisibilità in \mathbb{Z}

(3)

DEF. Siano $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$. Se esiste un intero q tale che $a = bq$ dico che

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

e scrivo
 $b|a$

ES. 3 è un fattore di 6

5 non è un divisore di 18 *

30 è un multiplo di -5

* Attenzione: in \mathbb{Q} (e in \mathbb{R}) 5 è un divisore di 18 poiché $18 = 5 \cdot \frac{18}{5}$.

Nei razionali (e nei reali) ogni numero $\neq 0$, essendo dotato di reciproco, è divisore (banale) di ogni altro. La teoria della divisibilità ha senso in \mathbb{Z} proprio perché in \mathbb{Z} ci sono solo due elementi dotati di reciproco:

$$1 \text{ e } -1: 1 \cdot 1 = 1, (-1) \cdot (-1) = 1$$

Nota: $b|a \iff b|(-a) \iff (-b)|a \iff (-b)|(-a)$

DIM:

$$b|a \Rightarrow a = bq_1 \Rightarrow -a = -(bq_1) = b(-q_1) \quad \text{-ecc.}$$

$$b|(-a) \Rightarrow -a = bq_2 \Rightarrow a = -(bq_2) = b(-q_2)$$

Teorema del quoziente e del resto (algoritmo della divisione)

4

Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici due interi q ed r t.c.

- $$1. a = bq + r$$
$$2. 0 \leq r < |b|$$

(ove $|b| = \begin{cases} b & \text{se } b > 0 \\ -b & \text{se } b < 0 \end{cases}$). q = quoziente; r = resto, nelle divisioni d'appr.

DIM.

Unicità: $a = bq + r$ con $0 \leq r < |b|$ } implicano:
 $a = b\bar{q} + \bar{r}$ con $0 \leq \bar{r} < |b|$ }
 $0 = b(q - \bar{q}) + (r - \bar{r}) \Rightarrow |r - \bar{r}| = |b| \cdot |q - \bar{q}| < |b|$
perché $|r - \bar{r}| < |b| \Rightarrow |q - \bar{q}| < 1 \Rightarrow q = \bar{q}$

Esistenza:

Si esaminano i 4 casi possibili

$a \geq 0 \text{ e } b > 0$; $a \geq 0 \text{ e } b < 0$; $a < 0, b > 0$; $a < 0, b < 0$

Cenni di dimostrazione del I . Gli altri su esempi.

Per induzione su a fissato b.

Passo iniziale dell'induzione: $a=0 \Rightarrow a=b \cdot 0 + 0$

$$\text{case } q=0, \lambda=0.$$

Se $a > 0$ e $a < b$ allora $a = b \cdot 0 + a$, cioè $q = 0, r = a$

Se $a \geq b$ allora $a - b \geq 0$ e posso applicare l'ipotesi

induttiva: $\exists \bar{q}, \bar{\pi}$ cosestic \leq b/ t.c.

$$a - b = b\bar{q} + \bar{e}$$

$$\Rightarrow a = b(\bar{q}+1) + \bar{r} \quad \text{such that } 0 \leq \bar{r} < |b| \quad \text{(*)}$$

Per il principio di riduzione è vera per ogni $a \geq 0$.

E' quel che c'è dietro l'algoritmo della divisione tra interi positivi:

$$\begin{array}{r} 273 \\ 53 \\ \hline 9 \end{array} \quad \left| \begin{array}{c} 11 \\ \hline 24 \end{array} \right.$$

$$273 = 11 \cdot 24 + 9$$

Significa "ho tolto 11" da 273 e poi da 262 ecc. per 24 volte, finché ho trovato un numero < 11

Caso $a \geq 0, b < 0$

$a = 32, b = -5$. Divido a per $|b|$:

$$32 = 5 \cdot 6 + 2 = (-5)(-6) + 2$$

$$q = -6, r = 2.$$

Caso $a < 0, b > 0$

$a = -32, b = 5$ mi ricordo al caso precedente:

$$32 = (-5) \cdot (-6) + 2$$

$$-32 = 5 \cdot (-6) - 2$$

$$-32 = 5 \cdot (-6) - 5 + (5 - 2)$$

$$-32 = 5 \cdot (-7) + 3$$

$$q = -7, r = 3.$$

moltiplico per -1:

Resto < 0! aggiungo e tolgo b:

→ se il resto forse zero non ci sarebbe problema

Caso $a < 0, b < 0$

$a = -32, b = -5$

mi ricordo al caso precedente, cambiando il segno del quoziente:

$$-32 = (-5) \cdot (+7) + 3$$

$$q = 7, r = 3.$$

NOTA : b divide a \Leftrightarrow il resto nella divisione di a per b è = 0.

Gli aggiustamenti sul resto servono solo se $r \neq 0$ e $a < 0$.

Massimo comune divisore di due interi $\neq 0$ (6)

DEF. Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Si dice max. com. divisore di a e b OGNI intero d t.c.

1. $d|a, d|b$

2. se $t \in \mathbb{Z} \setminus \{0\}$ è tale che $t|a$ e $t|b$
allora $t|d$.

L'algoritmo della divisione permette di arrivare a provare l'esistenza di $\text{M.C.D.}(a, b)$, ma attenzione:
se $d = \text{M.C.D.}(a, b)$ anche $-d = \text{M.C.D.}(a, b)$

Ancora: la nozione di M.C.D. è indipendente dall'ordine delle coppie a, b e dal segno dei due numeri:

$$\text{MCD}(12, 30) = \text{MCD}(30, -12) = \dots$$

e si può scegliere se assumere come MCD 6 oppure -6.

TEOR. (Algoritmo euclideo delle divisioni successive per la determinazione di $\text{M.C.D.}(a, b)$).

Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Esistono due interi x, y tali che

$$ax + by = d \text{ sia il M.C.D.}(a, b).$$

Visto quanto osservato sul segno di a e b , basta provare l'enunciato per $a > 0$ e $b > 0$ \rightarrow TESTO!

Qui illustriamo la dimostrazione su un esempio.
Supponiamo di voler trovare il MCD(3167, 281)

(7)

1. Divido il maggiore per il minore

$$3167 = 281 \cdot 11 + 46$$

$$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$

2. Divido il divisore b per il 1° resto r_1

$$281 = 76 \cdot 3 + 53$$

$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$

3. Divido il 1° resto per il 2° resto r_2

$$76 = 53 \cdot 1 + 23$$

$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$

4. Divido il 2° resto per il 3° resto r_3

$$53 = 23 \cdot 2 + 7$$

$$r_2 = r_3 q_4 + r_4 \quad 0 \leq r_4 < r_3$$

5. Divido il 3° resto per il 4° resto r_4

$$23 = 7 \cdot 3 + 2$$

$$r_3 = r_4 q_5 + r_5 \quad 0 \leq r_5 < r_4$$

6. Divido il 4° resto per il 5° resto r_5

$$7 = 2 \cdot 3 + 1$$

$$r_4 = r_5 q_6 + r_6 \quad 0 \leq r_6 < r_5$$

7. Divido il 5° resto per il 6° resto

$$2 = 1 \cdot 2 + 0$$

$$r_5 = r_6 \cdot q_7 + r_7, r_7 = 0$$

Dato che $r_7 = 0$ dico che $r_6 = 1$ è M.C.D.
di 3167 e 281.

Infatti $r_6 | r_5 \Rightarrow r_6 | r_4 = 7 = 3r_5 + r_6 \Rightarrow$

$$\Rightarrow r_6 | r_3 = 3r_4 + r_5 \Rightarrow r_6 | r_2 = 53 = 2r_3 + r_4 \Rightarrow$$

$$\Rightarrow r_6 | r_1 = 76 = 1r_2 + r_3 \Rightarrow r_6 | b = 281 = 3r_1 + r_2 \Rightarrow$$

$$\Rightarrow r_6 | a = 3167 = 11b + r_1 \quad \text{cioè } r_6 | a \in r_6 | b$$

Viceversa se $t | a$ e $t | b \Rightarrow t | r_1 = a - b \cdot 11 \Rightarrow$

$$\Rightarrow t | r_2 = b - 3r_1 \Rightarrow t | r_3 = r_1 - r_2 \cdot 1 \Rightarrow t | r_4 = r_2 - 2r_3 \Rightarrow$$

$$\Rightarrow t | r_5 = r_3 - 3r_4 \Rightarrow t | r_6 = r_4 - 3r_5.$$

Osservazioni

- 1) comunque si scelgano a e b l'algoritmo TERMINA poiché si crea una catena decrecente
- $$r_1 > r_2 > \dots > r_i > \dots \geq 0$$

di resti che sono numeri interi non negativi (dopo al più r_1 passi si arriva a zero) e quindi si trova M.C.D(a, b)

- 2) le due parti della dimostrazione sono basate sul fatto che se $k, m, n \in \mathbb{Z} \setminus \{0\}$ e $k|m, k|n$ allora, per ogni scelta di \bar{m}, \bar{n} in \mathbb{Z} si ha

$$k | \bar{m}m + \bar{n}n.$$

- 3) La seconda parte mostra che ogni resto può essere scritto attraverso a e b ; nell'esempio:

$$r_1 = a - 11b$$

$$r_2 = b - 3r_1 = -3a + 34b$$

$$r_3 = r_1 - r_2 = 4a - 45b$$

$$r_4 = r_2 - 2r_3 = -11a + 124b$$

$$r_5 = r_3 - 3r_4 = 37a - 417b$$

$$r_6 = r_4 - 3r_5 = -122a + 1375b$$

$x = -122$ e $y = 1375$ sono i due interi di cui il teorema proclama l'esistenza; in effetti

$$1 = -122 \cdot 3167 + 1375 \cdot 281. \quad \blacksquare$$

DEF. $a, b \in \mathbb{Z} \setminus \{0\}$ sono detti primi tra loro $\iff_{\text{DF}} \text{M.C.D.}(a, b) = 1$, cioè per quanto appena detto \iff esistono $x, y \in \mathbb{Z}$ tali che

$$ax + by = 1$$

Se $M.C.D(a,b) = d$ allora $-d$ è l'unico altro minimo comune divisore di a e b .

per definizione

$$1. \exists \bar{a}, \bar{b} \in \mathbb{Z} \text{ t.c. } a = d\bar{a}, b = d\bar{b}$$

$$\dots \underline{\text{e quindi}} \quad a = (-d)(-\bar{a}), \quad b = (-d)(-\bar{b})$$

$$2. \text{ Se } t \in \mathbb{Z} \text{ è tale che } \exists a', b' \in \mathbb{Z} \text{ con}$$

$$a = ta', \quad b = tb' \text{ allora } \exists d' \text{ t.c. } d = td'$$

$$\dots \underline{\text{e quindi}} \text{ tale che } (-d) = td'$$

$$\text{dunque } -d = M.C.D.(a,b)$$

Non esistono altri $M.C.D(a,b)$ poiché se $d \neq \bar{d}$ sono $M.C.D(a,b)$ allora $d \neq 0, \bar{d} \neq 0$ e

$$\left. \begin{array}{l} \exists d' \text{ t.c. } d = d'\bar{d} \\ \exists d'' \text{ t.c. } \bar{d} = d''d \end{array} \right\} \Rightarrow d = d'd''d \Rightarrow d'd''=1$$

e poiché $d', d'' \in \mathbb{Z}$ può essere solo $d' = d'' = 1$
 $\circ d' = d'' = -1$. ■

Cancello duale di $M.C.D(a,b)$: minimo comune multiplo.

DEF. $a, b \in \mathbb{Z} \setminus \{0\}$. Un intero m è detto m.c.m.(a,b)

se

$$1. a|m, b|m$$

$$2. \text{ se } t \in \mathbb{Z} \text{ è tale che } a|t \text{ e } b|t \text{ allora } m|t$$

Si prova che se d è un $M.C.D(a,b)$ allora

$$m = \frac{a \cdot b}{d}$$

è un m.c.m.(a,b) e $-m$ è l'unico altro minimo comune multiplo di a e b .

Numeri primi e teorema di fattorizzazione

(9)

DEF. Un numero $p \in \mathbb{Z} \setminus \{0, 1, -1\}$ si dice primo se ogni volta che divide il prodotto di due interi a, b divide almeno uno dei due:
 $p | ab$ e $p \nmid a \Rightarrow p | b$.

Ad es. 6 non è un numero primo perché divide $30 = 2 \cdot 15$ ma non divide né 2 né 15.

Si dimostra che questo concetto è equivalente al concetto di numero irriducibile:

DEF. Un numero $p \in \mathbb{Z} \setminus \{0, 1, -1\}$ si dice irriducibile se è divisibile solo per $\pm p$ e per ± 1 .

[Se p è irriducibile e non divide a $M.C.D.(p, a) = 1$
 $\Rightarrow \exists x, y \in \mathbb{Z}$ t.c. $1 = xp + ya \Rightarrow b = xp^2 + yab \Rightarrow$
 \Rightarrow se $p | ab$ deve dividere $b \Rightarrow p$ è primo]

Se p è primo e d un suo divisore, esiste $q \in \mathbb{Z}$ tale che $p = dq \Rightarrow p$ divide il prodotto $dq \Rightarrow$ divide almeno uno dei due fattori che può essere suoi divisori \Rightarrow se divide d : $d = \pm p$ e $q = \pm 1$
" " " : $q = \pm p$ e $d = \pm 1$

L'importanza di tali numeri risiede nel fatto che ogni numero intero può essere scritto in modo unico, a meno dell'ordine dei fattori e dei segni a questi attribuiti, come prodotto di numeri primi.

TEOR di fattorizzazione "unica". (o fondamentale
dell'aritmetica) (10)

Sia $z \in \mathbb{Z} \setminus \{0, 1, -1\}$. Esistono $s \geq 1$ numeri primi (non necessariamente distinti) p_1, p_2, \dots, p_s tali che

$$z = p_1 \cdot p_2 \cdot \dots \cdot p_s.$$

Questa scomposizione in fattori primi è sostanzialmente unica nel senso che se q_1, q_2, \dots, q_t sono numeri primi tali che

$$z = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

si ha $s=t$ ed è possibile riordinare i fattori in modo che

$$p_1 = \pm q_1, p_2 = \pm q_2, \dots, p_s = \pm q_s.$$

Ad es.

$$\begin{aligned} -18 &= (-3) \cdot 3 \cdot 2 = 3 \cdot 3 \cdot (-2) = (-3) \cdot (-3) \cdot (-2) = \dots \\ &= 3^2 \cdot (-2) = (-3)^2 \cdot (-2): \end{aligned}$$

Si possono cioè raccogliere i fattori uguali (uso della proprietà commutativa del prodotto) e quindi si vede che

ogni $z \in \mathbb{Z} \setminus \{0, 1, -1\}$ ha una fattorizzazione essenzialmente unica come prodotto di potenze di primi distinti p_1, \dots, p_r con opportune potenze $\alpha_1, \dots, \alpha_r$ tutte > 0 :

$$z = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

di è detta molteplicità del fattore p_i nella scomposizione di z in fattori primi.

Nell'esempio: 3 è un fattore di molteplicità 2 di 18, (-2) è un fattore di molteplicità 1.

Coseguenze :

1) $a, b \in \mathbb{Z} \setminus \{0, 1, -1\}$

b è un divisore di a se e solo se ogni primo^p che compare nella fattorizzazione in primi di b compare anche in quella di a e la molteplicità di p in b è \leq di quella in a .

Ad esempio $18 = 2 \cdot 3^2$ è un divisore di $270 = 2 \cdot 3^3 \cdot 5$.

In particolare M.C.D. (a, b) è il prodotto delle potenze dei primi che compaiono in entrambe le fattorizzazioni, con la molteplicità minore tra le due.

Ad esempio se $a = 270 = 2 \cdot 3^3 \cdot 5$

$$b = 2475 = 3^2 \cdot 5^2 \cdot 11, \quad \text{M.C.D}(270, 2475) = 3^2 \cdot 5 = 45.$$

VERIFICARLO CON L'ALGORITMO EUCLideo

Similmente m.c.m. (a, b) è il prodotto delle potenze dei primi che compaiono in almeno una fattorizzazione, con la molteplicità maggiore tra le due.

Ad esempio se $a = 270, b = 2475$

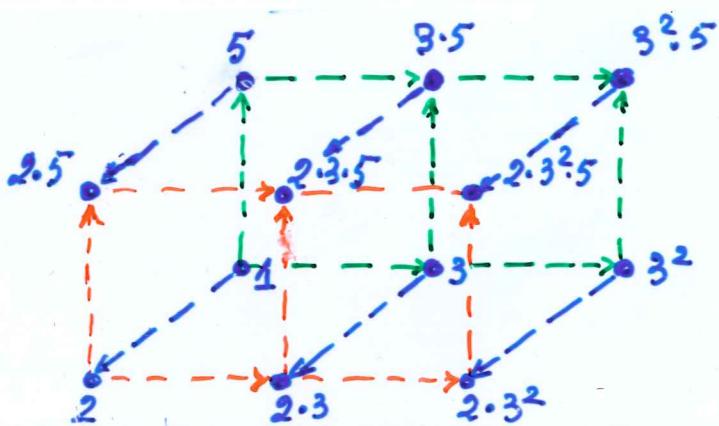
$$\text{m.c.m.}(270, 2475) = 2 \cdot 3^3 \cdot 5^2 \cdot 11 = 6 \cdot 6 = \dots$$

2) Se $z = p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_r^{d_r}$ si possono contare i divisori di z : $(d_1+1)(d_2+1) \cdot \dots \cdot (d_r+1)$.

Tutti nella scomposizione di un divisore di z il fattore p_i può comparire un numero di volte compreso tra 0 e d_i . (tra i divisori vengono conteggiati anche 1 e z)

(12)

Ad esempio i possibili divisori di $90 = 2 \cdot 3^2 \cdot 5$
 sono $2 \cdot 3 \cdot 2 = 12$:



3) L'insieme P dei numeri primi di \mathbb{Z} non è finito

Infatti se i numeri primi positivi distinti fossero n : p_1, p_2, \dots, p_n , il numero intero $m = (p_1, p_2, \dots, p_n) + 1$ non sarebbe divisibile per alcuno dei numeri primi ma nemmeno un numero primo (poiché non sta in P) e questo contraddice il teor. di fattorizzazione.



Le questioni su M.C.D. e fattorizzazione sono state qui presentate come conseguenza o comunque come strettamente correlate con l'algoritmo della divisione e il conseguente algoritmo euclideo.