Ratio Math. n. 7 - 1994
111 - 123

TEORIA DELLA DIVISIBILITÀ E ALGORITMO EUCLIDEO NELL'INSEGNAMENTO NELLE SCUOLE SUPERIORI

Antonio Maturo - Fabiola Paccapelo** - Loredana Renzullo**
**Dipartimento di Scienza, Storia dell'Architettura e Restauro*
Università "G. D'Annunzio" viale Pindaro, 42 - Pescara
***Liceo Scientifico "L. Da Vinci" via Collemarino - Pescara*

Sommario. Si presenta una proposta per introdurre la teoria della divisibilità nelle Scuole Medie Superiori. Nel primo paragrafo si richiama la divisibilità in $\mathcal{N}$ evidenziando le proprietà da generalizzare ed il concetto di norma. Nel secondo paragrafo si danno le proprietà che riteniamo fondamentali per presentare nelle scuole la divisibilità in un anello integro, con particolare riferimento a quelli normati ed euclidei. Negli esempi si mettono bene in luce le differenze fra elementi primi ed elementi irriducibili e quindi l'importanza dell'algoritmo euclideo.

1. DIVISIBILITÀ IN $\mathcal{N}$

Sia $\mathcal{N} = \{0, 1, 2, \ldots\}$ l'insieme dei naturali.

Definizione 1.1 (Divisibilità)

Siano $a, b \in \mathcal{N}$. Diciamo che a divide b oppure che a è un divisore di b e scriviamo $a|b$ se:

$$\exists\, c \in \mathcal{N} : b = ca.$$

Poniamo $\forall\, a, b \in \mathcal{N}$,

$$a \circledS b \Leftrightarrow \begin{cases} b = 0 \\ b \neq 0,\ a \neq 0,\ a \leq b \end{cases}$$

Proposizione 1.1

La relazione $\circledS$ in $\mathcal{N}$ è di ordine totale con 1 elemento minimo e 0 elemento massimo.

Proposizione 1.2

La relazione $|$ in $\mathcal{N}$ è di ordine parziale, con 1 elemento minimo e 0 elemento massimo, ossia:

$$1|b \quad e \quad b|0 \qquad \forall\, b \in \mathcal{N}.$$

Proposizione 1.3

$a|b \Rightarrow a \leqslant b$, ossia la $|$ è una restrizione di $\leqslant$.

Proposizione 1.4

Il numero 1 ha un solo divisore; ogni $a \neq 1$ ha almeno 2 divisori: 1 ed a.

Il numero 0 ha infiniti divisori; ogni $a \neq 0$ ha un numero finito di divisori, non superiori ad a.

Definizione 1.2

Sia $p \in \mathcal{N} - \{0, 1\}$. Diciamo che p è *irriducibile* o *indecomponibile* o *primo* se:

$$a|p \Rightarrow (a = 1 \text{ oppure } a = p)$$

Definizione 1.3

Siano $a, b \in \mathcal{N}$. Diciamo che $d \in \mathcal{N}$ è un *massimo comune divisore* tra a e b se:

(D1) $$d|a, d|b$$

(D2) $$(c|a, c|b) \Rightarrow c|d$$

Proposizione 1.5

$\forall a, b \in \mathcal{N}$ esiste al più un massimo comun divisore di a e b indicato con D(a, b).

Dim.: d e d' massimi comuni divisori di a e $b \Rightarrow (d|d' \text{ e } d'|d) \Rightarrow$
$\Rightarrow (d \leq d', d' \leq d) \Rightarrow d = d'$

Proposizione 1.6

$\forall a \in \mathcal{N}$, $D(a, 0) = a$, $D(a, 1) = 1$

Proposizione 1.7

$$\left.\begin{array}{l} \exists\, D(b, r) \\ a = bx + r \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \exists\, D(a, b) \\ D(a, b) = D(b, r) \end{array}\right.$$

Dim.: $(d = D(b, r), a = bx + r) \Rightarrow (d|b, d|r) \Rightarrow (d|a, d|b)$;

$$(c|a, c|b, r = a - bx) \Rightarrow c|r, c|b \Rightarrow c|d.$$

Teorema 1.1

Per ogni $a, b \in \mathcal{N}$, $b \neq 0$ esiste una unica coppia ordinata (q, r) di elementi di $\mathcal{N}$, detti rispettivamente *quoziente* e *resto* della divisione di a per b e indicati con $quot(a, b)$, $rest(a, b)$ tali che:

(DR1) $$a = bq + r$$

(DR2) $$0 \leq r < b$$

Proposizione 1.8

Per ogni $a, b \in \mathcal{N}$, $b \neq 0$, poniamo $r = rest(a, b)$.
Si ha:

$$d = D(b, r) \Rightarrow d = D(a, b)$$

$$r = 0 \Rightarrow D(a, b) = b$$

Dim.: segue dalle prop. 1.6 e 1.7

Teorema 1.2 (Algoritmo euclideo)

Per ogni $a, b \in \mathcal{N}$, $b \neq 0$, esiste una successione finita $\{r_1, r_2, \ldots, r_n\}$, $n \geq 2$ di elementi di $\mathcal{N}$ tali che:

posto $$a = r_0, \quad b = r_1,$$

(AE1) $$r_i > 0 \quad \forall i < n \quad e \quad r_n = 0$$

(AE2) $$r_i = rest\,(r_{i-2}, \quad r_{i-1})$$

(AE3) $$D(a, b) = r_{n-1}$$

Corollario del teorema 1.2

Per ogni $a, b \in \mathcal{N}$ esiste ed è unico il massimo comun divisore di a e b.

Teorema 1.3

Per ogni $a, b \in \mathcal{N}$ e $\forall\, m \in \mathcal{N} - \{0\}$, $a \mid b \Leftrightarrow am \mid bm$

$$d = D(a, b) \Leftrightarrow md = D(ma, mb)$$

Teorema 1.4 (Combinazione lineare)

Per ogni $a, b \in \mathcal{N}$ esistono h e $k \in \mathcal{Z}$ tali che, posto $d = D(a, b)$,

$$d = ah + bk.$$

Inoltre

$$d = \min \{|ah + bk|, h \in \mathcal{Z}, k \in \mathcal{Z}\}.$$

Definizione 1.4

Per ogni $a, b \in \mathcal{N}$, si dice che a e b sono *primi fra loro* se $D(a, b) = 1$.

Corollario del Teorema 1.4

$$a \text{ e } b \text{ primi fra loro } \Leftrightarrow \exists\, h, k \in \mathcal{Z} : 1 = ah + bk.$$

Teorema 1.5 (Fondamentale della teoria della divisibilità).

$$\text{Per ogni } a, b \in \mathcal{N}\ (k \mid ab,\ D(k, a) = 1) \Rightarrow k \mid b$$

Dim. $(D(k, a) = 1) \Rightarrow (D(kb, ab) = b) \Rightarrow (k \mid kb,\ k \mid ab \Rightarrow k \mid b)$

Teorema 1.6

$$\text{Per ogni } a \in \mathcal{N}_1,\ p \text{ primo } \Rightarrow (p \perp a \Leftrightarrow D(p, a) = 1)$$

Dim. (p primo, $p \perp a$) $\Leftrightarrow$ (p primo e solo 1 è tale che $1 \mid p$ e $1 \mid a$)

Teorema 1.7

Per ogni $a, b \in \mathcal{N}$
p primo $\Leftrightarrow p \mid a \cdot b \Leftrightarrow p \mid a$ o $p \mid b$)

Dim.: ($\Rightarrow$) (p primo, $p \mid ab$, $p \perp a$) $\Rightarrow$ ($p \mid ab$, $D(p, a) = 1$) $\Rightarrow p \mid b$
($\Leftarrow$)(p non primo) $\Rightarrow (\exists\, r, s,\ 1 < r, s < p : p \mid r \cdot s,\ p \perp r,\ p \perp s)$

Teorema 1.8 (Fondamentale dell'aritmetica)

Ogni $a \in \mathcal{N} - \{0, 1\}$ si può esprimere in un unico modo come prodotto $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$ con i p_i fattori primi tali che $p_1 < p_2 \ldots < p_n$ e $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n \in \mathcal{N} - \{0\}$

2. DIVISIBILITÀ IN UN DOMINIO DI INTEGRITÀ

Sia $\mathcal{A}$ un anello commutativo unitario.

Definizione 2.1 (Divisibilità)

Siano $a, b \in \mathcal{A}$.

Diciamo che a *divide* b oppure che a è una divisore di b e scriviamo $a \mid b$ se $\exists\, c \in \mathcal{A} : b = c \cdot a$.

Teorema 2.1

La relazione $\mid$ è un preordine in $\mathcal{A}$, ossia è riflessiva e transitiva.

Se $b \in \mathcal{A}$ ed x è un elemento invertibile di $\mathcal{A}$ risulta $x \mid b, b \mid 0$.

Definizione 2.2

Si dice che a e $b \in \mathcal{A} - \{0\}$ sono *divisori dello zero* "complementari fra loro" se $a \cdot b = 0$.

Un anello privo di divisori dello zero si dice *dominio di integrità* o *anello integro.*

Definizione 2.3

Due elementi a e $b \in \mathcal{A}$ si dicono *associati* se $a \mid b$ e $b \mid a$.

Teorema 2.2

Sia a un dominio di integrità. Allora

(a associato a b) $\Leftrightarrow$ ($\exists\, c \in \mathcal{A}$, c invertibile : $a = c \cdot b$)

Teorema 2.3

La relazione in $\mathscr{A}$, $a \ominus b$ se e solo se a è associato a b è una relazione di equivalenza. Essa determina una partizione in classi di associati.

Se $\mathscr{A}$ è un dominio di integrità, detta $[a]$ la classe degli associati ad $a \in \mathscr{A}$, risulta:

$$[a] = \{x \in \mathscr{A} : \exists\, c \text{ invertibile } \in \mathscr{A} \text{ tale che } x = c \cdot a\}.$$

Teorema 2.4

Sia $\mathscr{D}(a)$ l'insieme dei divisori di $a \in \mathscr{A}$. Allora:

$$a \ominus b \Leftrightarrow D(a) = D(b).$$

Teorema 2.5

Ogni elemento invertibile $a \in \mathscr{A}$ è tale che $\mathscr{D}(a) = [1]$.

Ogni elemento non invertibile b di un dominio di integrità è tale che:

$$\mathscr{D}(b) \supseteq [1] \cup [b] \quad \text{con} \quad [1] \cap [b] \neq \emptyset$$

Definizione 2.4

Si dice *norma* in $\mathscr{A}$ ogni funzione $v : \mathscr{A} \to \mathscr{N}$ tale che

(N1) $$v(a) = 0 \Leftrightarrow a = 0$$

(N2) $$v(a \cdot b) = v(a) \cdot v(b).$$

Teorema 2.6

Esiste una norma in $\mathscr{A}$ se e solo se $\mathscr{A}$ è un dominio di integrità.

Dim. Se $a \cdot b = 0$, $a \neq 0$, $b \neq 0$ e valgono (N1) ed (N2) si ha:

$$v(a \cdot b) = v(0) = 0 \text{ e } v(a \cdot b) = v(a) \cdot v(b) \neq 0. \quad \text{Assurdo.}$$

La $v(0) = 0$, $v(a) = 1$ per $a \neq 0$ è una norma se $\mathscr{A}$ è un dominio d'integrità.

Supponiamo, da ora in poi, che $\mathscr{A}$ sia un dominio di integrità e che v sia una norma in $\mathscr{A}$.

Teorema 2.7

$a \mid b \Rightarrow v(a) \mid v(b)$ in $\mathcal{N}$

Dim.: $b = ca \Rightarrow v(b) = v(c) \cdot v(a)$

Corollario al teorema 2.7

$a \sim b \Rightarrow v(a) = v(b)$

a invertibile $\Rightarrow v(a) = 1$

Dim.: $a \sim b \Rightarrow v(a) \mid v(b)$ e $v(b) \mid v(a)$

$v(1) = v(1 \cdot 1) = v(1) \cdot v(1) \Rightarrow v(1) = 1$

Definizione 2.5

Sia $p \in \mathcal{A} - ([0] \cup [1])$. Diciamo che p è *indecomponibile* o *irriducibile* se:

$$a \mid p \Rightarrow (a \in [1] \text{ oppure } a \in [p])$$

Diciamo che $p \in \mathcal{A} - \{[0] \cup [1]\}$ è *primo* se, $\forall\, a, b \in \mathcal{A}$

$$p \mid a \cdot b \Leftrightarrow p \mid a \text{ o } p \mid b.$$

Teorema 2.8

Se p è primo in $\mathcal{A}$ allora è anche irriducibile.

Dim.: Sia p primo e sia $a \in \mathcal{A}$ tale che $a \mid p$.

Allora $\exists\, k \in \mathcal{A} \mid p = k \cdot a$.

Essendo p primo $p \mid a$ o $p \mid k$.

Poiché $k \mid p$ e $a \mid p$ uno fra k e a è un associato di p e l'altro è un elemento invertibile. Segue che $a \in [1]$ o $a \in [p]$ e quindi che p è irriducibile.

Definizione 2.6

Siano $a, b \in \mathcal{A}$. Diciamo che $d \in \mathcal{A}$ è un *massimo comun divisore* tra a e b se

(D1) $$d|a,\ d|b$$

(D2) $$(c|a\ ,\ c|b) \Rightarrow c|d.$$

Teorema 2.9

Per ogni $a, b \in \mathscr{A}$ se d è un massimo comun divisore tra a e b sono tali tutti e soli gli elementi di [d].

Sia $\mathscr{D}(a, b)$ eventualmente vuoto, l'insieme dei massimi comuni divisori di a e b.

Teorema 2.10

Per ogni $a \in \mathscr{A}$ e per ogni c invertibile $\in \mathscr{A}$

$$D(a, 0) = [a], \qquad D(a, c) = [1].$$

Teorema 2.11

$$\left.\begin{matrix} D(b, r) \neq \emptyset \\ a = bx + r \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} D(a, b) \neq \emptyset \\ D(a, b) = D(b, r) \end{matrix}\right.$$

Definizione 2.7

La norma v in $\mathscr{A}$ si dice *euclidea* se soddisfa la

(N3) $\forall\ a, b \in \mathscr{A}, \quad b \neq 0, \quad \exists\ q, r \in \mathscr{A}$ tali che:

(DR1) $$a = bq + r$$

(DR2) $$0 \leq v(r) < v(b).$$

Se v è euclidea, $\mathscr{A}$ si dice *dominio di integrità euclideo.*

Teorema 2.12 (Algoritmo euclideo)

Per ogni $a, b \in \mathscr{A}$, $b \neq 0$, se v è una norma euclidea esiste una successione finita $\{r_1, r_2, \ldots\ldots r_n\}$, $n \geq 2$, di elementi di $\mathscr{A}$ tali che posto $a = r_0$, $b = r_1$:

(AE1) $$v(r_i) > 0 \quad \forall\ i < n \quad e \quad v(r_n) = 0$$

(AE2) $$\exists\ q_i \in \mathscr{A} : r_{i-2} = q_i\, r_{i-1} + r_i,\ v(r_i) < v(r_{i-1})$$

(AE3) $$D(a, b) = [r_{n-1}].$$

Definizione 2.8

Sia $\mathscr{A}$ un anello.

Per ogni $a \in \mathscr{A} - ([0] \cup [1]$, si dice *fattorizzazione* di a ogni successione finita $\{a_0, a_1, a_2, \ldots\ldots, a_n\}$ di elementi di $\mathscr{A}$ con $n \geq 1$ tali che:

(F_1) $\qquad a_0 \in [1]$

(F_2) $\qquad a_i$ è primo, $\quad \forall\, i \in \{1, 2, \ldots\ldots, n\}$

(F_3) $\qquad a = a_0\ a_1\ a_2 \ldots\ldots\ a_n$

Definizione 2.9

Per ogni $a \in \mathscr{A} - ([0] \cup [1])$, due fattorizzazioni

$$\mathscr{S}_1 = \{a_0\ a_1\ a_2 \ldots\ldots\ a_n\} \quad \text{e} \quad \mathscr{S}_2 = \{b_0\ b_1\ b_2 \ldots\ldots\ b_m\}$$

si dicono *equivalenti* se esiste una biiezione φ di $\mathscr{S}_1$ in $\mathscr{S}_2$ tale che:

$$[a_i] = [\varphi(a_i)], \qquad \forall\, i \in \{0, 1, 2, \ldots\ldots, n\}.$$

(In particolare $n = m$).

Teorema 2.13 [cfr. [1]].

Sia $\mathscr{A}$ un anello euclideo. Per ogni $a \in \mathscr{S} - [[0] \cup [1]]$, esiste almeno una fattorizzazione di a e se $\mathscr{S}_1$ ed $\mathscr{S}_2$ sono due fattorizzazioni di a, allora $\mathscr{S}_1$ è equivalente ad $\mathscr{S}_2$.

Teorema 2.14

Sia $\mathscr{A}$ un anello euclideo. Un elemento di $\mathscr{A}$ è irriducibile se e solo se è primo.

3. ESEMPI ED ESERCIZI

3.1 *Caso con due fattorizzazioni non equivalenti*

Si consideri il dominio di integrità:

$$H(3) = \left\{z \in \mathbf{C} : z = a + ib\sqrt{3}, \quad a \in \mathscr{N}, b \in \mathscr{N}\right\}$$

risulta

$$4 = (1 + i\sqrt{3})(1 - i\sqrt{3}) \quad \text{e} \quad 4 = 2 \cdot 2$$

Le due fattorizzazioni di 4 *non sono equivalenti.*
Gli elementi:

$$2, \quad 1 + i\sqrt{3}, \quad 1 - i\sqrt{3} \qquad \text{sono irriducibili in H (3).}$$

Essi, però, non sono primi. Infatti:

$$2 \mid (1 + i\sqrt{3})(1 - i\sqrt{3}) \quad \text{ma} \quad 2 \nmid (1 + i\sqrt{3}) \quad \text{e} \quad 2 \nmid (1 - i\sqrt{3}).$$

3.2 *Esempi di domini di integrità dotati di norma*

Per ogni $c \in \mathcal{N} - \{0\}$, consideriamo l'insieme H(c) dei numeri complessi:

$$z = a + ib\sqrt{c} \qquad \text{con } a, b \in \mathcal{N}$$

H(c), rispetto alle usuali operazioni di addizione e moltiplicazione in $\mathcal{C}$ forma un *dominio d'integrità.*

La *norma* di $z = a + ib\sqrt{c}$ è il numero:

$$N(z) = z \cdot z', \quad \text{con} \quad z' = a - ib\sqrt{c} \quad \text{(coniugato di z)}$$

Precisamente:

$$N(z) = a^2 + b^2c.$$

Si ha che

$$N(z) \in \mathcal{N} \text{ e inoltre}$$

1) $$N(z) = 0 \Leftrightarrow z = 0$$

2) $$\forall z_1, z_2 \in \mathcal{A}\,; \quad N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$$

3.3 *Divisione con il resto in H(c)*

(a) Teoria. **Teorema [cfr. [1]]**

Siano u e $v \in H(c)$, con $v \neq 0$. Esistono, in H (c) due elementi q ed r, detti *quoziente e resto della divisione* di u per v, tali che:

$[D_1]$ $$u = vq + r$$

$[D_2]$ $$N(r) \leq (1 + c)\, N(v) \,|\, 4.$$

Per $c \leq 2$, $N(r) < N(v)$ per cui H(c) è un anello euclideo.

Per $c = 3$ dalla $[D_2]$ segue $N(r) \leq N(v)$.

(b) Come si calcolano q, r, N(r)

Si ha che $u = vq + r \Rightarrow uv' = vv'q + v'r$ e $vv' = N(v) \in \mathcal{N}$. Allora si divide uv' per N(v) come in $\mathcal{Z}$, considerando separatamente la parte reale e quella immaginaria e ottenendo q e v'r.

Poniamo $$r^* = v'r.$$

Essendo $$N(r^*) = N(v'r) = N(v') \cdot N(r),$$

si ottiene $$N(r) = N(r^*) \,|\, N(v').$$

Inoltre da $$r^* = v'r,$$

si ottiene $$vr^* = vv'r, \quad vr^* = N(v)r,$$

$$r = \frac{1}{N(v)}\, vr^*.$$

(c) Esempio

Dividiamo $u = 7 + i8\sqrt{2}$ per $v = 4 + i7\sqrt{2}$.

Si ha: $uv' = 140 - i\,17\sqrt{2}$, $N(v) = 114$

Sia $q = \text{quot}(uv', 114)$, $r^* = \text{rest}(uv', 114)$.

Si ottiene $q = 1, \quad r^* = 26 - i17\sqrt{2}.$

Segue $N(r^*) = 1254, \quad N(r) = 1254 : 114 = 11,$

$$r = \frac{v}{N(v)} \quad r^* = \frac{1}{114}\left(4 + i7\sqrt{2}\right)\left(26 - i17\sqrt{2}\right) =$$

$$= \frac{1}{114}\left(342 + i114\sqrt{2}\right) = 3 + i\sqrt{2}.$$

Notiamo che $N(r) = 11 \ll N(v) = 114$

(d) Un altro esempio

Dividiamo 2 per $1 + i\sqrt{3}$.

Si ha $u = 2\,, \quad v = 1 + i\sqrt{3}$

$$N(v) = 4\,, \quad uv' = 2\left(1 - i\sqrt{3}\right) = 2 - 2i\sqrt{3}\,,$$

$$q = -i\sqrt{3}\,, \quad r^* = 2 + 2i\sqrt{3}\,, \quad N(r^*) = 16, \quad \text{da cui}$$

$$N(r) = N(r^*) \,|\, N(v) = 4, \quad \text{ossia} \quad N(r) = N(v).$$

3.4 Un esempio in cui $\mathscr{D}(a, b) = \emptyset$

In H(3) sia

$$a = 4, \qquad b = 2\left(1 + i\sqrt{3}\right)$$

Risulta che $D(a, b) \neq \emptyset.$

Infatti se $d \in \mathscr{D}(a, b)$ si ha $(z|a,\ z|b) \Rightarrow z|d.$

Allora $1 + i\sqrt{3}$ e 2 dividono d.

I divisori di b sono $1,\ 2,\ 1+i\sqrt{3}\ ,\ b$ e poiché:

$$2 \nmid (1+i\sqrt{3}) \quad \text{e} \quad (1+i\sqrt{3}) \nmid 2,$$

deve essere $d = b.$

Allora: $b = 2(1+i\sqrt{3}) \mid 4,$

ossia $1+i\sqrt{3} \mid 2,$ assurdo.

BIBLIOGRAFIA

[1] A. MATURO – B. RIZZI, *Sulla decomposizione di un numero primo in somma di tre quadrati* Periodico di Matematiche n° 3 – 1990.

[2] A. MATURO – B. RIZZI, *Sulla decomposizione di un numero naturale in somma di quadrati* Periodico di Matematica n° 4 – 1990

[3] A. WEIL – *Teoria dei numeri* Einaudi 1993