

## divisori dello zero in $Z_n$

**OSSERVAZIONE 1** In  $Z_n$  può accadere che il prodotto di due elementi diversi da zero sia uguale a zero, cioè che non valga la *legge di annullamento del prodotto*. Per esempio, in  $Z_6$  risulta  $[2][3] = [0]$  ed è  $[2] \neq [0]$  e  $[3] \neq [0]$ .

**DEFINIZIONE 2** Un elemento  $a \in Z_n$  si dice *divisore dello zero* se esiste un elemento  $b \neq 0$  tale che  $ab = 0$ .

**PROPOSIZIONE 3** Un elemento  $a \in Z_n$  è divisore dello zero se, e solo se,  $a$  ed  $n$  non sono coprimi.

**DIM.** Se  $a$  ed  $n$  non sono coprimi, per  $d = MCD(a, n)$ , abbiamo  $1 < d \leq n$ , così  $b = n/d$  è minore di  $n$  e risulta  $ab = 0$  in  $Z_n$ . Se  $ab = 0$ , con  $0 < a, b < n$ , allora  $n$  non divide  $a$ , non divide  $b$  e divide  $ab$ ; ne segue che  $MCD(a, n) \neq 1$ .

**ESERCIZIO 4** Provare che in  $Z_n$  vale la legge di annullamento del prodotto se, e solo se, l'intero  $n$  è primo.

## teorema di Fermat-Eulero

**TEOREMA 5** Siano  $a, n$  due interi positivi coprimi con  $n > 1$ . Allora risulta

$$a^{\Phi(n)} \equiv 1 \pmod{n}. \quad (1)$$

**DIM.** Cominciamo con l'osservare che, se  $y \in U(n)$  e poniamo

$$yU(n) = \{yx \quad : \quad x \in U(n)\},$$

risulta  $yU(n) = U(n)$ . Posto, allora,  $k = \Phi(n)$ , sia

$$U(n) = \{x_1, x_2, \dots, x_k\}$$

e poniamo  $y = x_1 x_2 \cdots x_k$ . Poiché  $a \in U(n)$  e  $aU(n) = U(n)$ , in  $Z_n$  abbiamo

$$y = x_1 x_2 \cdots x_k = (ax_1)(ax_2) \cdots (ax_k) = a^k y.$$

Essendo  $y$  invertibile in  $U(n)$ , possiamo moltiplicare l'ultima uguaglianza per  $y^{-1}$  e otteniamo che

$$1 = a^k$$

in  $Z_n$ , come volevamo dimostrare.

**OSSERVAZIONE 6** Il teorema di Fermat-Eulero, asserendo che

$$aa^{\Phi(n)-1} = a^{\Phi(n)} \equiv 1 \pmod{n}$$

quando l'intero  $a$  é coprimo con  $n$ , può anche riformularsi dicendo che in  $Z_n$ , se un elemento  $b$  é invertibile, risulta  $b^{-1} = b^{\Phi(n)-1}$ . Questa osservazione chiarisce che il calcolo dell'inverso di  $b$  in  $Z_n$  attraverso la (1) richiede la conoscenza di  $\Phi(n)$  e, quindi, della fattorizzazione in primi di  $n$ .

## piccolo teorema di Fermat

**TEOREMA 7** Sia  $p$  un primo positivo. Allora risulta

$$a^p \equiv a \pmod{p}, \quad \text{per ogni intero positivo } a; \quad (2)$$

o, equivalentemente,

$$a^{p-1} \equiv 1 \pmod{p}, \quad \text{per ogni intero positivo } a \text{ non divisibile per } p. \quad (3)$$

**DIM.** Se  $p$  non divide  $a$ , abbiamo  $\Phi(p) = p - 1$  e quindi  $a^{p-1} = a^{\Phi(p)}$ . Ne segue, per il teorema di Fermat-Eulero, che  $a^{p-1} \equiv 1 \pmod{p}$  e quindi  $a^p \equiv a \pmod{p}$ . Se  $p$  divide  $a$ , la (2) é banale.

**COROLLARIO 8** Se  $p$  é un primo positivo e  $b$  un elemento non nullo di  $Z_p$ , risulta

$$b^{-1} = b^{p-2}; \quad (4)$$

o, equivalentemente,

$$a^{p-1} \equiv 1 \pmod{p}, \quad \text{per ogni intero positivo } a < p. \quad (5)$$

**OSSERVAZIONE 9** Il piccolo teorema di Fermat, per ogni intero positivo  $a < m$ , dá una condizione necessaria (che nell'antica Cina, per  $a = 2$ , si riteneva fosse anche sufficiente) affinché un intero positivo  $m > 1$  sia primo:

$$m \text{ primo} \Rightarrow m \mid (a^m - a).$$

Purtroppo queste condizioni non sono sufficienti e i primi due controesempi, per  $a = 2$ , sono  $m = 341 = 11 \cdot 31$  (diciottesimo secolo) e  $m = 561 = 3 \cdot 11 \cdot 17$ . Gli interi  $m > 1$  che verificano il "test cinese" per un fissato  $a$ , cioè tali che  $m \mid (a^m - a)$ , prendono il nome di *pseudoprimi* in base  $a$ . Più in generale si ha che il piccolo teorema di Fermat non é invertibile e, quindi, non può essere utilizzato come test di primalità. Esistono, infatti, interi non primi  $m > 1$ , divisibili per  $a^m - a$ , per ogni intero positivo  $a < m$ . Questi sono noti come *numeri di Carmichael* e i primi due esempi sono 561 e  $1729 = 7 \cdot 13 \cdot 19$ .

## congruenze lineari

Se  $a, b, m$  sono interi con  $m > 1$ , l'equazione in  $x$

$$ax \equiv b \pmod{m} \quad (6)$$

prende il nome di *equazione congruenziale lineare*, o *congruenza lineare*, e una sua soluzione é, per definizione, un intero  $\bar{x}$  tale che  $a\bar{x} \equiv b \pmod{m}$ . L'essere  $\bar{x}$  una soluzione della (6) equivale all'esistenza di un intero  $n$  tale che  $a\bar{x} - b = nm$ , cioè  $a\bar{x} - mn = b$ . Allora abbiamo:

**PROPOSIZIONE 10** La congruenza lineare (6) ha soluzioni se, e solo se,  $MCD(a, m)$  divide  $b$ .

**PROPOSIZIONE 11** Nell'ipotesi che l'equazione (6) abbia una soluzione  $c$ , poniamo  $d = MCD(a, m)$  e  $m = dm_1$ . Allora le soluzioni della (6) sono tutte e sole quelle del tipo

$$\bar{x} = c + nm_1, \quad n \in \mathbb{Z}. \quad (7)$$

**PROPOSIZIONE 12** Nell'ipotesi che l'equazione (6) sia risolubile, poniamo  $d = MCD(a, m)$ ,  $m = dm_1$  e sia  $c$  una sua soluzione. Allora, le soluzioni della (6) a due a due incongrue modulo  $m$  sono esattamente  $d$  e precisamente:

$$c, c + m_1, c + 2m_1, \dots, c + (d - 1)m_1. \quad (8)$$

**DIM.** E' chiaro che le soluzioni (8) sono a due a due incongrue modulo  $m$ . Sia, dunque,  $c + nm_1$  una soluzione della (6) e sia  $n = dq + r$ , con  $q, r$  quoziente e resto della divisione di  $n$  per  $d$ . Allora é  $0 \leq r < d$ ,

$$c + nm_1 = c + (dq + r)m_1 = c + dqm_1 + rm_1 =$$

$$c + qm + rm_1 \equiv c + rm_1 \pmod{m}$$

e l'asserto é completamente provato.

## teorema cinese del resto

**TEOREMA 13** Siano  $m_1, m_2$  interi maggiori di 1 e coprimi. Allora il sistema di congruenze lineari

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases} \quad (9)$$

ammette soluzioni, che risultano a due a due congruenti modulo  $m_1 m_2$ . Più precisamente, se  $c$  è una soluzione del sistema, le sue soluzioni sono tutti e soli gli interi del tipo  $c + nm_1 m_2$ , con  $n \in \mathbb{Z}$ .

**DIM.** Gli interi  $m_1$  e  $m_2$  sono invertibili rispettivamente in  $\mathbb{Z}_{m_2}$  e  $\mathbb{Z}_{m_1}$ . Esistono, quindi, due interi  $c_1$  e  $c_2$  tali che  $c_1 m_2 \equiv 1 \pmod{m_1}$  e  $c_2 m_1 \equiv 1 \pmod{m_2}$ . Allora, l'intero

$$c = b_1 c_1 m_2 + b_2 c_2 m_1$$

è una soluzione del sistema (9), avendosi

$$c = b_1 c_1 m_2 + b_2 c_2 m_1 \equiv b_1 c_1 m_2 \pmod{m_1} \equiv b_1 \pmod{m_1}$$

e

$$c = b_1 c_1 m_2 + b_2 c_2 m_1 \equiv b_2 c_2 m_1 \pmod{m_2} \equiv b_2 \pmod{m_2}.$$

Ora, se  $c$  è una fissata soluzione del sistema (9), sono soluzioni anche gli interi del tipo  $c + nm_1 m_2$ , con  $n \in \mathbb{Z}$ . Inoltre, se  $\bar{c}$  è un'ulteriore soluzione, si ha che  $\bar{c} - c$  è divisibile per  $m_1 m_2$ , essendo  $m_1$  e  $m_2$  coprimi, e quindi  $\bar{c} = c + nm_1 m_2$ , per un opportuno intero  $n$ . L'asserto è così completamente provato.

## teorema cinese del resto

**TEOREMA 14** Siano  $m_1, m_2, \dots, m_t$  interi maggiori di 1 e a due a due coprimi. Allora il sistema di congruenze lineari

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_t \pmod{m_t} \end{cases} \quad (10)$$

ammette soluzioni, che risultano a due a due congruenti modulo  $m_1 m_2 \cdots m_t$ . Più precisamente, se  $c$  é una soluzione del sistema, le sue soluzioni sono tutti e soli gli interi del tipo

$$c + nm_1 m_2 \cdots m_t, \text{ con } n \in \mathbb{Z}.$$

## esempi di operazioni

- Addizione e moltiplicazione in  $N_o, Z, Q, R, C$ .
- Addizione e moltiplicazione in  $Z_n$ .
- Moltiplicazione in  $U(n)$ .
- Addizione in uno spazio vettoriale.
- Divisione in  $Q^*, R^*, C^*$ .
- Addizione in  $M_{m,n}(A)$ ,  $A = N_o, Z, R, C$ .
- Moltiplicazione righe per colonne in  $M_n(A)$ ,  $A = N_o, Z, R, C$ .
- Addizione e moltiplicazione nell'insieme dei polinomi a coefficienti in  $N_o, Z, Q, R, C$ .
- Massimo comune divisore e minimo comune multiplo in  $N$ .
- Unione e intersezione in  $P(S)$ .
- Differenza simmetrica in  $P(S)$ .
- Composizione in  $Sym(S)$ .
- Moltiplicazione di uno scalare per un vettore in uno spazio vettoriale.

**OSSERVAZIONE 15** Tutte le operazioni elencate si presentano come delle leggi che permettono di individuare un elemento di un insieme a partire da una coppia elementi assegnati. E' pertanto ragionevole pensare che la nozione di *operazione* possa generalizzarsi ed esprimersi in termini precisi nel linguaggio della teoria degli insiemi.

## operazioni e strutture algebriche

**DEFINIZIONE 16** Un'applicazione di  $S \times S$  in  $S$  prende il nome di *operazione interna ad  $S$* . Assegnata un'operazione  $\star : S \times S \rightarrow S$ , si pone, per ogni  $a, b \in S$ ,

$$\star(a, b) = a \star b.$$

L'elemento  $a \star b$  di  $S$  si chiama *composto* di  $a$  e  $b$  mediante  $\star$ .

### notazioni piú usate

- la notazione *additiva*: si usa il segno "+" e il composto di due elementi  $a, b$  si denota con  $a + b$ ;
- la notazione *moltiplicativa*: si usa il segno "." o "x" e il composto di due elementi  $a, b$  si denota con  $a \cdot b$  o  $a \times b$ , o anche con  $ab$ ;
- la notazione *esponenziale*: il composto di due elementi  $a, b$  si denota con  $a^b$ .

**DEFINIZIONE 17** Sia  $A$  un insieme non vuoto,  $A \neq S$ . Un'applicazione di  $A \times S$  in  $S$  prende il nome di *operazione esterna ad  $S$  con dominio di operatori  $A$* .

**DEFINIZIONE 18** Si chiama *struttura algebrica ad  $n$  operazioni su  $S$*  ogni  $(n + 1)$ -pla del tipo

$$(S, \star_1, \star_2, \dots, \star_n),$$

ove ogni  $\star_i$  é una operazione su  $S$  (interna o esterna). L'insieme  $S$  si chiama *sostegno* della struttura. Una struttura algebrica si dice *finita* (risp. *infinita*) se il suo sostegno é un insieme finito (risp. infinito). Se una struttura algebrica é finita, il numero di elementi del suo sostegno si chiama *ordine* della struttura; nel caso contrario si dice che la struttura ha *ordine infinito*.

## esempi di strutture algebriche

- $(N_o, +), (Z, +), (Q, +), (R, +), (C, +)$ .
- $(N_o, \cdot), (Z, \cdot), (Q, \cdot), (R, \cdot), (C, \cdot)$ .
- $(N_o, +, \cdot), (Z, +, \cdot), (Q, +, \cdot), (R, +, \cdot), (C, +, \cdot)$ .
- $(Z[x], +, \cdot), (Q[x], +, \cdot), (R[x], +, \cdot), (C[x], +, \cdot)$ .
- $(Z_n, +), (Z_n, \cdot), (Z_n, +, \cdot), (U(n), \cdot)$ .
- $(P(S), \cap), (P(S), \cup), (P(S), \cup, \cap)$ .
- $(S, \wedge), (S, \vee), (S, \wedge, \vee)$ , ove  $(S, \leq)$  é un reticolo.

## alcune proprietà delle operazioni

- Proprietá *commutativa*:

$$a \circ b = b \circ a, \quad \text{per ogni } a, b \in S.$$

- Proprietá *associativa*:

$$a \circ (b \circ c) = (a \circ b) \circ c, \quad \text{per ogni } a, b, c \in S.$$

- Proprietá *distributiva (a destra)* di  $\circ$  rispetto a  $\star$  :

$$(a \star b) \circ c = (a \circ c) \star (b \circ c), \quad \text{per ogni } a, b, c \in S.$$

## elemento neutro

**DEFINIZIONE 19** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Un elemento  $u \in S$  si dice *neutro* se

$$u \circ a = a \circ u = a, \text{ per ogni } a \in S.$$

Una struttura  $(S, \circ)$  con elemento neutro si dice *unitaria*.

**ESERCIZIO 20** Provare che, se  $(S, \circ)$  possiede un elemento neutro, questo é unico.

**DEFINIZIONE 21** In notazione moltiplicativa l'elemento neutro si chiama *unitá* e si denota con 1. In notazione additiva l'elemento neutro si chiama *zero* e si denota con 0.

### esempi

- $(A, +)$ ,  $A = N_o, Z, Q, R, C, Z_n$ , ha 0 come elemento neutro.
- $(A^*, \cdot)$ ,  $A = N_o, Z, Q, R, C, Z_n$ , ha 1 come elemento neutro.
- Sia  $/$  l'operazione di divisione in  $Q^*$ .  $(Q^*, /)$  (struttura non associativa e non commutativa) non possiede elemento neutro.
- $(P(S), \cap)$  ha  $S$  come l'elemento neutro.
- $(P(S), \cup)$  ha  $\emptyset$  come l'elemento neutro.

**ESERCIZIO 22** Sia  $(S, \leq)$  un reticolo. Dire sotto quali condizioni  $(S, \wedge)$  e  $(S, \vee)$  posseggono l'elemento neutro.

## elementi simmetrizzabili

**DEFINIZIONE 23** Sia  $(S, \circ)$  una struttura algebrica dotata di elemento neutro  $u$ . Un elemento  $a \in S$  si dice *simmetrizzabile* se esiste  $a' \in S$  tale che

$$a' \circ a = a \circ a' = u .$$

L'elemento  $a'$  si chiama *simmetrico* di  $a$ .

**OSSERVAZIONE 24** In una una struttura algebrica  $(S, \circ)$  dotata di elemento neutro  $u$  si ha:

- $a'$  simmetrico di  $a \Leftrightarrow a$  simmetrico di  $a'$ .
- L'elemento neutro  $u$  é simmetrizzabile e si ha  $u' = u$ .

**DEFINIZIONE 25** Nella notazione moltiplicativa il simmetrico di un elemento  $a$  si chiama *inverso* di  $a$  e si denota con  $a^{-1}$ . Nella notazione additiva il simmetrico di  $a$  si chiama *opposto* di  $a$  e si denota con  $-a$ .

### ESEMPI 26

- In  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}_n, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  tutti gli elementi sono simmetrizzabili.
- In  $(\mathbb{Z}, \cdot)$ ,  $1$  e  $-1$  sono gli unici elementi simmetrizzabili.
- In  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{C}^*, \cdot)$  tutti gli elementi sono simmetrizzabili.
- In  $(\mathbb{Z}[x], +)$ ,  $(\mathbb{Q}[x], +)$ ,  $(\mathbb{R}[x], +)$ ,  $(\mathbb{C}[x], +)$  tutti gli elementi sono simmetrizzabili.
- Una matrice  $A$  appartenente a  $(M_n(\mathbb{Q}), \cdot)$ , o  $(M_n(\mathbb{R}), \cdot)$  o  $(M_n(\mathbb{C}), \cdot)$  é simmetrizzabile se, e solo se,  $\det(A) \neq 0$ .

**ESERCIZIO 27** Provare che una matrice  $A$  in  $(M_2(\mathbb{Z}), \cdot)$  é simmetrizzabile se, e solo se,  $\det(A) = \pm 1$ .

**DEFINIZIONE 28** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Un sottoinsieme non vuoto  $X$  di  $S$  si dice *parte stabile* se:

$$a \circ b \in X, \text{ per ogni } a, b \in X.$$

**OSSERVAZIONE 29** Quando  $X$  é una parte stabile, la restrizione dell'operazione " $\circ$ " a  $X \times X$  é una operazione interna ad  $X$ ; abbiamo cosí una nuova struttura algebrica  $(X, \circ)$ , che si dice *indotta* su  $X$  da  $(S, \circ)$ .

**DEFINIZIONE 30** Sia  $(S, \circ)$  una struttura algebrica con operazione esterna e dominio di operatori  $A$ . Un sottoinsieme non vuoto  $X$  di  $S$  si dice *parte stabile* se:

$$a \circ x \in X, \text{ per ogni } x \in X \text{ e } a \in A.$$

Anche in questo caso abbiamo una struttura indotta  $(X, \circ)$ .

**ESEMPI 31**

- L'insieme degli interi pari é stabile in  $(\mathbb{Z}, +, \cdot)$ .
- L'insieme degli interi dispari non é stabile in  $(\mathbb{Z}, +)$  e in  $(\mathbb{Z}, +, \cdot)$ .
- L'insieme  $n\mathbb{Z}$  costituito dai multipli di un fissato intero  $n \neq 0$  é una parte stabile in  $(\mathbb{Z}, +, \cdot)$ .
- Gli insiemi  $\{0, 1\}$  e  $\{0, 1, -1\}$  sono stabili in  $(\mathbb{Z}, \cdot)$  ma non sono stabili in  $(\mathbb{Z}, +)$ .
- $\mathbb{Z}$  é stabile in  $(\mathbb{Q}, +, \cdot)$ .  $\mathbb{Q}$  é stabile in  $(\mathbb{R}, +, \cdot)$ .  $\mathbb{R}$  é stabile in  $(\mathbb{C}, +, \cdot)$ .
- I numeri complessi di modulo 1 sono una parte stabile di  $(\mathbb{C}, \cdot)$  ma non sono una parte stabile di  $(\mathbb{C}, +)$ .
- Le matrici diagonali d'ordine  $n$  sono una parte stabile dell'anello  $M_n(F)$ ,  $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .
- Le matrici scalari d'ordine  $n$  sono una parte stabile dell'anello  $M_n(F)$ ,  $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .