

interi modulo n

Sia n un intero e consideriamo la relazione d'equivalenza in Z cosí definita:

$$a\mathfrak{R}_n b \Leftrightarrow a - b = hn, \text{ per qualche intero } h \in Z.$$

La relazione \mathfrak{R}_n si chiama *congruenza modulo n* . Per indicare che é $a\mathfrak{R}_n b$ si scrive anche $a \equiv b(\text{mod } n)$ e si legge *a é congruo*, o *congruente*, a b modulo n .

DEFINIZIONE 1 L'insieme quoziente Z/\mathfrak{R}_n si denota con Z_n , o con Z/nZ , e si chiama *insieme degli interi modulo n* . La classe d'equivalenza di un elemento $a \in Z$ rispetto ad \mathfrak{R}_n si denota con $[a]_{\mathfrak{R}_n}$ o piú semplicemente con $[a]$.

Nel seguito supporremo sempre $n > 1$ perché:

- $n = 0 \Rightarrow \mathfrak{R}_0$ é la relazione di uguaglianza in Z .
- $n = 1 \Rightarrow a\mathfrak{R}_1 b, \forall a, b \in Z \Rightarrow [a]_{\mathfrak{R}_1} = [b]_{\mathfrak{R}_1} = Z, \forall a, b \in Z$;
- $\mathfrak{R}_n = \mathfrak{R}_{-n}$;

Valgono le seguenti proprietá e osservazioni:

- $[0] = \{hn : h \in Z\}$ (questo insieme si denota anche con nZ).
- $a \neq 0 \Rightarrow [a] = \{a + hn : h \in Z\}$ (questo insieme si denota anche con $a + nZ$).
- $0 \leq a < n \Rightarrow n - a \equiv -a(\text{mod } n)$.
- $r = \text{resto della divisione tra } a \text{ ed } n \Rightarrow a \equiv r(\text{mod } n)$.
- Il numero delle *classi di congruenza modulo n* é esattamente n e risulta

$$Z_n = \{[0], [1], \dots, [n - 1]\}.$$

interi modulo n

OSSERVAZIONE 2 In molti testi il resto r della divisione di a per n é denotato col simbolo $a \bmod n$. In questo caso le scritture $b = a \bmod n$ e $b \equiv a \bmod n$ hanno significato diverso: la prima dice che é $b = r$, la seconda che $b - a$ é un multiplo di n .

Altre due importanti proprietá sono:

- $x, x' \in [a], y, y' \in [b] \Rightarrow [x + y] = [x' + y']$.
- $x, x' \in [a], y, y' \in [b] \Rightarrow [xy] = [x'y']$.

In Z_n risultano *ben definite* le operazioni:

$$[a] + [b] = [a + b] \quad , \quad [a][b] = [ab].$$

Queste operazioni verificano le seguenti *proprietá fondamentali*:

- $([a] + [b]) + [c] = [a] + ([b] + [c])$,
- $[a] + [0] = [0] + [a] = [a]$,
- $[a] + [-a] = [0]$,
- $[a] + [b] = [b] + [a]$,
- $([a][b])[c] = [a]([b][c])$,
- $[a][1] = [1][a] = [a]$,
- $[a][b] = [b][a]$,
- $([a] + [b])[c] = [a][c] + [b][c]$,

anello degli interi modulo n

OSSERVAZIONE 3 Z_n , rispetto alle operazioni di addizione e moltiplicazione, é un *anello commutativo unitario* nel quale lo zero é $[0]$ e l'*unitá* é $[1]$.

TABELLE DI CAYLEY DI Z_2

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

TABELLE DI CAYLEY DI Z_3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

TABELLE DI CAYLEY DI Z_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

TABELLE DI CAYLEY DI Z_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

esercizi

OSSERVAZIONE 4 L'aritmetica modulo 2 si presta a svariate applicazioni perché è riproducibile mediante i due possibili stati di alcuni sistemi fisici per i quali il passaggio da uno stato all'altro è regolato dall'addizione o dalla moltiplicazione in \mathbb{Z}_2 .

ESERCIZIO 5 Sia

$$n = r_m 10^m + r_{m-1} 10^{m-1} + \dots + r_2 10^2 + r_1 10 + r_0.$$

Provare che risulta $n \equiv r_m + r_{m-1} + \dots + r_2 + r_1 + r_0 \pmod{9}$.

SOLUZIONE Si ha:

$$\bullet 10^m - 1 = \underbrace{999 \dots 9}_{m \text{ volte}} = 9 \cdot 10^{m-1} + 9 \cdot 10^{m-2} + \dots + 9 \cdot 10^2 + 9 \cdot 10 + 9$$

$$\Rightarrow 10^m - 1 \equiv 0 \pmod{9}.$$

$$\bullet n - (r_m + r_{m-1} + \dots + r_2 + r_1 + r_0) =$$

$$(r_m 10^m + \dots + r_1 10 + r_0) - (r_m + \dots + r_1 + r_0) =$$

$$(10^m - 1)r_m + \dots + (10^2 - 1)r_2 + (10 - 1)r_1 \equiv 0 \pmod{9}.$$

ESERCIZIO 6 Dimostrare i seguenti criteri di divisibilità:

- un intero è divisibile per 2 se, e solo se, la sua ultima cifra decimale è pari;
- un intero è divisibile per 3 se, e solo se, la somma delle sue cifre decimali è divisibile per 3;
- un intero è divisibile per 4 se, e solo se, l'intero corrispondente alle sue ultime due cifre decimali è divisibile per 4;

esercizi

ESERCIZIO 7 Trovare il resto della divisione per 9 di un intero del tipo 83^{6a} .

SOLUZIONE Si tratta di trovare l'unico intero r compreso fra 0 e 9 tale che

$$83^{6a} \equiv r \pmod{9}.$$

Poiché é

$$83 \equiv 2 \pmod{9},$$

risulta

$$83^{6a} \equiv 2^{6a} \pmod{9}.$$

D'altra parte, essendo

$$2^{6a} = (2^6)^a \quad \text{e} \quad 2^6 \equiv 1 \pmod{9},$$

abbiamo

$$2^{6a} \equiv 1 \pmod{9}.$$

Ne segue che

$$83^{6a} \equiv 1^a \equiv 1 \pmod{9},$$

cosí il resto cercato é 1.

funzione di Eulero

DEFINIZIONE 8 Per un intero $n > 1$ si denota con $\Phi(n)$ il numero degli interi positivi minori di n e coprimi con esso. La funzione Φ si chiama *funzione di Eulero*.

ESERCIZIO 9 Provare che $\Phi(n) = n - 1$ se, e solo se, n é primo.

PROPOSIZIONE 10 Per ogni primo positivo p e per ogni intero $h > 0$, risulta

$$\Phi(p^h) = p^h - p^{h-1}. \quad (1)$$

DIM. Gli interi positivi minori di p^h che non sono coprimi con p^h sono tutti e soli quelli del tipo mp , con $1 \leq m \leq p^{h-1}$, e da ciò segue l'asserto.

PROPOSIZIONE 11 Se p e q sono primi positivi distinti, risulta

$$\Phi(p^h q^k) = \Phi(p^h) \Phi(q^k) = p^h q^k \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right),$$

per ogni $h, k \in \mathbb{N}$.

COROLLARIO 12 Se a, b sono due interi positivi coprimi, risulta

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

PROPOSIZIONE 13 Sia $n > 1$ un intero e siano p_1, p_2, \dots, p_h i primi positivi che dividono n . Allora risulta

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_h}\right). \quad (2)$$

DIM. É un corollario delle due precedenti proposizioni.

elementi invertibili in Z_n

Denotiamo con Z_n^* l'insieme degli elementi non nulli di Z_n .

DEFINIZIONE 14 Un elemento $a \in Z_n^*$ si dice *invertibile* se esiste un elemento $b \in Z_n^*$ tale che $ab = 1$. In questo caso b si chiama *inverso* di a e si denota con a^{-1} . L'insieme degli elementi invertibili di Z_n si denota con $U(n)$.

TEOREMA 15 Un elemento $a \in Z_n^*$ é invertibile se, e solo se, a ed n sono coprimi in Z .

DIM. Si ha:

• $ax = 1$ in $Z_n \Rightarrow ax \equiv 1(\text{mod } n) \Rightarrow ax - 1 = hn$, per qualche $h \in Z \Rightarrow ax - hn = 1 \Rightarrow \text{MCD}(a, n) = 1$.

• $\text{MCD}(a, n) = 1 \Rightarrow ha + kn = 1$, per qualche $h, k \in Z \Rightarrow ha - 1 = -kn \Rightarrow ha \equiv 1(\text{mod } n) \Rightarrow ha = 1$ in Z_n .

COROLLARIO 16 Il numero degli elementi invertibili di Z_n^* é uguale a $\Phi(n)$.

COROLLARIO 17 Gli elementi di Z_n^* sono tutti invertibili se, e solo se, n é un primo. In tal caso Z_n é un campo.

OSSERVAZIONE 18 Se a ed n sono coprimi, il calcolo di a^{-1} in Z_n puó effettuarsi andando a trovare una soluzione (b, h) in Z dell'equazione

$$ax + ny = 1.$$

Per (b, h) , infatti, risulta $ab = 1 - nh$; cioè $b = a^{-1}$ in Z_n . Facciamo presente che esistono algoritmi efficienti per risolvere la precedente equazione.

ESERCIZIO 19 Provare che il prodotto di due elementi di $U(n)$ é un elemento di $U(n)$.