

Congruenze in \mathbb{Z} ; l'insieme quoziente \mathbb{Z}/\equiv_n

Per ogni $n \in \mathbb{Z}$, si consideri in \mathbb{Z} la relazione, che per il momento denoteremo con $(n\mathbb{Z})$, così definita:

$$a (n\mathbb{Z}) b \Leftrightarrow n \text{ divide } a-b$$

Esempio: $5 (7\mathbb{Z}) 19$, perché $7 \mid 5-19=-14$, mentre 4 non è nella relazione $(5\mathbb{Z})$ con 8 , perché 5 non divide $4-8=-4$.

Osservazione 1: Si noti che $x (0\mathbb{Z}) y$ se, e solo se, $x = y$, mentre risulta $x (1\mathbb{Z}) y$, per ogni coppia (x,y) di interi. Dunque, la relazione $(0\mathbb{Z})$ è l'uguaglianza, mentre la relazione $(1\mathbb{Z})$ coincide con la relazione totale. Infine, poiché $n \mid x-y$ se, e solo se, $-n \mid x-y$, la relazione $(n\mathbb{Z})$ coincide con quella $(-n\mathbb{Z})$, per cui non si perderà di generalità quando si considererà la relazione $(n\mathbb{Z})$, con $n \geq 0$.

Teorema 1 La relazione $(n\mathbb{Z})$ è una relazione di equivalenza in \mathbb{Z} , per ogni $n \in \mathbb{Z}$.

Dim. Occorre verificare che $(n\mathbb{Z})$ è riflessiva, simmetrica e transitiva. Da $n \mid a-a=0$ segue $a (n\mathbb{Z}) a$, per ogni $a \in \mathbb{Z}$, per cui $(n\mathbb{Z})$ è riflessiva. Se $x (n\mathbb{Z}) y$, da $n \mid x-y$ segue $n \mid -(x-y) = y-x$, per cui risulta $y (n\mathbb{Z}) x$, e $(n\mathbb{Z})$ è simmetrica. Infine, se $x (n\mathbb{Z}) y$ e $y (n\mathbb{Z}) z$, da $n \mid x-y$ e $n \mid y-z$ discende $n \mid (x-y)+(y-z) = x-z$, e quindi $x (n\mathbb{Z}) z$.

La relazione di equivalenza $(n\mathbb{Z})$ è detta **congruenza modulo n** , e sarà denotata da ora in poi con il simbolo \equiv_n . Se $a (n\mathbb{Z}) b$, scriveremo dunque $a \equiv_n b$, oppure $a \equiv b \pmod{n}$, e leggeremo **a congruo b (modulo n)**.

Le classi di equivalenza relative alla relazione \equiv_n sono dette **classi resto degli interi modulo n** , o anche **interi modulo n** . La classe dell'elemento a sarà denotata con la scrittura $[a]_n$ o anche, quando ciò non dia adito ad ambiguità, con la scrittura $[a]$.

L'insieme quoziente $\mathbb{Z}/\equiv_n = \{ [a] \mid a \in \mathbb{Z} \}$ è detto l'**insieme delle classi resto degli interi modulo n** , o l'**insieme degli interi modulo n** , e può essere anche denotato con il simbolo \mathbb{Z}_n .

Proposizione 2 Siano $a, n \in \mathbb{Z}$. Allora $[a]_n = \{ a+nk : k \in \mathbb{Z} \}$.

Dim Sussistono le seguenti uguaglianze: $[a]_n = \{ x \in \mathbb{Z} : x \equiv_n a \} = \{ x \in \mathbb{Z} : n \text{ divide } x-a \}$
 $= \{ x \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } x-a = nk \} = \{ x \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } x = a+nk \} = \{ a+nk : k \in \mathbb{Z} \}$.

Osservazione 3 Si noti che, alla luce della proposizione precedente, risulta, qualunque sia $n \in \mathbb{Z}$, $[0]_n = \{ nk : k \in \mathbb{Z} \}$, cioè la classe dello 0 coincide con l'insieme dei multipli di n . Si ricorda che tale insieme si denota con il simbolo $n\mathbb{Z}$. Similmente, per ogni intero a , con $a+n\mathbb{Z}$ si indica l'insieme $\{ a+nk : k \in \mathbb{Z} \}$. La prop.2 si può riformulare dicendo che $[a]_n = a+n\mathbb{Z}$, per ogni $a, n \in \mathbb{Z}$.

Vogliamo ora studiare l'insieme quoziente \mathbb{Z}_n . Alla luce di quanto notato nell'Osservazione 1, sarà possibile limitarci ad esaminare il caso $n \geq 0$. Inoltre, essendo la \equiv_0 l'uguaglianza, sarà sufficiente supporre $n > 0$.

Se indichiamo con la scrittura $rest(x, n)$ il resto della divisione dell'intero x per l'intero $n > 0$, vale la seguente proposizione:

Proposizione 4 Siano $x, y \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Risulta allora.

- i) $x \equiv rest(x, n) \pmod{n}$;
- ii) gli interi $0, 1, 2, \dots, n-1$ sono a due a due incongrui \pmod{n}
- iii) $x \equiv y \pmod{n} \Leftrightarrow rest(x, n) = rest(y, n)$.

Dim. i) Esiste $q \in \mathbb{Z}$ tale che $x = nq + rest(x, n)$, per cui $x - rest(x, n) = nq$ è divisibile per n .
ii) Siano r, s interi tali che $0 \leq r \leq s \leq n-1$, e si supponga $s \equiv r \pmod{n}$. Allora $s-r$ è un multiplo di n tale che $0 \leq s-r \leq n-1$, e di qui segue $s-r = 0$, e $s = r$.
iii) Sia $x \equiv y \pmod{n}$; da $rest(x, n) \equiv_n x$, $x \equiv_n y$, $y \equiv_n rest(y, n)$ segue $rest(x, n) \equiv_n rest(y, n)$, ed essendo $0 \leq rest(x, n), rest(y, n) \leq n-1$ risulta $rest(x, n) = rest(y, n)$. Il viceversa segue subito da i).

Dalla prop.4 segue subito il seguente

Teorema 5 Se $n \geq 1$ è un intero, risulta $\mathbb{Z} / \equiv_n = \{ [0], [1], [2], \dots, [n-1] \}$, e gli elementi $[0], [1], [2], \dots, [n-1]$ di \mathbb{Z} / \equiv_n sono a due a due distinti. In particolare \mathbb{Z} / \equiv_n ha ordine n .

Dim. Dalla i) della prop.4 segue che, se $a \in \mathbb{Z}$, $[a] = [\text{rest}(a,n)]$. Da $0 \leq \text{rest}(a,n) \leq n-1$ si deduce facilmente che $\mathbb{Z} / \equiv_n = \{ [a] / a \in \mathbb{Z} \} = \{ [0], [1], [2], \dots, [n-1] \}$. L'essere poi gli elementi $[0], [1], [2], \dots, [n-1]$ di \mathbb{Z} / \equiv_n a due a due distinti segue invece dalla ii) della prop.4.

Osservazione 6 Il teorema precedente fornisce un modo semplice per rappresentare le n classi distinte che costituiscono \mathbb{Z}_n , ma non l'unico. Risulta infatti, per esempio, $\mathbb{Z}_5 = \{ [0], [1], [2], [3], [4] \} = \{ [5], [-4], [7], [13], [-1] \}$.

La struttura quoziente $(\mathbb{Z}_n, +, \cdot)$

La congruenza \equiv_n è compatibile (cfr. cap.3, §17) con le ordinarie operazioni di somma e prodotto definite in \mathbb{Z} . Vale infatti la seguente

Proposizione 7 Siano a, b, c, d numeri interi relativi, sia $n \in \mathbb{N}^*$, e si supponga $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$. Allora risulta $a+c \equiv b+d \pmod{n}$, $ac \equiv bd \pmod{n}$.

Dim. Per ipotesi esistono $h, k \in \mathbb{Z}$ tali che $a-b = hn$, $c-d = kn$. Ne segue $(a-b)+(c-d) = hn+kn$, ovvero $(a+c)-(b+d) = (h+k)n$, e quindi $a+c \equiv b+d \pmod{n}$.

Per quel che riguarda il prodotto, da $a-b = hn$ segue $(a-b)c = hnc$, ovvero $ac-bc = hnc$. Analogamente risulta $bc-bd = b(c-d) = bkn$, da cui segue $ac-bd = (ac-bc)+(bc-bd) = hnc+bkn = (hc+bk)n$, e quindi $ac \equiv bd \pmod{n}$, come si voleva.

La proposizione precedente ci assicura che è possibile definire nell'insieme quoziente \mathbb{Z}_n le operazioni quoziente relative alle ordinarie operazioni di somma e prodotto definite in \mathbb{Z} , ponendo, per ogni $[a], [b] \in \mathbb{Z}_n$

$$[a]+[b] = [a+b]$$

$$[a][b] = [ab]$$

La struttura quoziente $(\mathbb{Z}_n, +, \cdot)$ risulta essere, al pari di $(\mathbb{Z}, +, \cdot)$, un anello commutativo unitario, che è detto l'anello delle classi resto modulo n (cfr. cap.4, §24, §27). Non tutte le proprietà di $(\mathbb{Z}, +, \cdot)$ sono però ereditate da $(\mathbb{Z}_n, +, \cdot)$: per esempio, mentre in \mathbb{Z} non ci sono divisori dello 0, in \mathbb{Z}_4 , pur essendo $[2] \neq [0]$, risulta $[2][2] = [0]$; ancora, mentre in \mathbb{Z}

gli unici elementi invertibili rispetto al prodotto sono $+1$ e -1 , in \mathbb{Z}_5 la classe $[2]$, che è distinta da $[1]$ e da $[-1]$, risulta invertibile, in quanto $[2][3] = [6] = [1]$.

Nelle proposizioni che seguono si vedrà in che modo si possono determinare l'invertibilità e la regolarità di una classe $[a] \in \mathbb{Z}_n$, e di conseguenza alcune proprietà di $(\mathbb{Z}_n, +, \cdot)$.

Proposizione 8 Siano $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Allora $[a]$ è invertibile in \mathbb{Z}_n se, e solo se, a ed n sono primi tra loro.

Dim. Se $[a]$ è invertibile, esiste $[b] \in \mathbb{Z}_n$ tale che $[a][b] = [ab] = [1]$; quindi $n \mid 1-ab$, ossia esiste $h \in \mathbb{Z}$ tale che $1-ab = hn$. Da $1 = ab+hn$ segue che a ed n sono primi tra loro (cfr. cap.1, §4) .

Viceversa, supposti a ed n primi tra loro, essendo $1 = \text{M.C.D.}(a,n)^{(*)}$, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha a + \beta n$ (cfr. cap.1, §4); da $\alpha a - 1 = -\beta n$ segue allora $\alpha a \equiv 1 \pmod{n}$, per cui $[\alpha a] = [\alpha][a] = [1]$, e $[\alpha]$ è l'inverso di $[a]$.

(*) Da ora e nel seguito, se a e b sono interi non entrambi nulli, si indicherà con $\text{M.C.D.}(a,b)$ l'unico massimo comun divisore positivo tra a e b .

Proposizione 9 Siano $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$, e sia $[a] \neq [0]$. Allora $[a]$ è un divisore dello 0 in \mathbb{Z}_n se, e solo se, a ed n non sono primi tra loro.

Dim. Se $[a]$ è un divisore dello 0 non è regolare, quindi non è invertibile. Per la proposizione precedente a ed n non sono primi tra loro.

Viceversa, se $d = \text{M.C.D.}(a,n)$, risulta $1 < d < n$ (non può essere $d = n$, poiché è $[a] \neq [0]$), ed esistono $a_1, n_1 \in \mathbb{Z}$ tali che $a = a_1 d$, $n = n_1 d$. Dall'essere $1 < n_1 < n$ segue $[n_1] \neq [0]$, e $[a][n_1] = [a_1 d n_1] = [a_1][n] = [a_1][0] = [0]$, per cui $[a]$ è un divisore dello 0.

Corollario 10 Siano $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$, e sia $[a] \neq [0]$. Allora $[a]$ è invertibile se, e solo se, non è un divisore dello 0.

Nella proposizione che segue si evidenzia come la struttura dell'anello \mathbb{Z}_n è intimamente legata alla natura dell'intero n :

Proposizione 11 Sia $n > 1$ un intero. Allora le seguenti affermazioni sono equivalenti:

- i) l'anello \mathbb{Z}_n è un campo;
- ii) l'anello \mathbb{Z}_n è un dominio d'integrità;
- iii) n è un numero primo.

Dim. Le condizioni i) e ii) sono equivalenti per il corollario 10. Per dimostrare l'equivalenza di i) e ii), si osservi che, se n è primo, tutti gli interi $1, 2, \dots, n-1$ sono primi con n , e quindi tutte le classi $[1], [2], \dots, [n-1]$ sono invertibili. Viceversa, supposto che \mathbb{Z}_n sia un campo, se n non fosse primo esisterebbe un divisore n_1 di n tale che $1 < n_1 < n$; allora risulterebbe $[n_1] \neq [0]$ ed $[n_1]$ non invertibile, essendo $\text{M.C.D.}(n_1, n) = n_1 > 1$. Dall'assurdo segue che n è necessariamente primo.

Esempio Gli anelli $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_{11}$ sono dei campi, mentre l'anello \mathbb{Z}_{12} non è un dominio d'integrità: l'insieme dei suoi elementi invertibili rispetto al prodotto è $U(\mathbb{Z}_{12}) = \{ [1], [5], [7], [11] \}$, mentre l'insieme dei suoi divisori dello 0 è $\{ [2], [3], [4], [6], [8], [9], [10] \}$.

Equazioni congruenziali

Nel paragrafo precedente è stata data una condizione necessaria e sufficiente affinché una classe $[a] \neq [0]$ sia invertibile. In questa sezione si vedrà come è possibile determinare $[a]^{-1}$ quando $[a]$ è invertibile.

Si noti che, se $[a] \in \mathbb{Z}_n$, $[a]$ è invertibile se, e solo se, esiste $[c] \in \mathbb{Z}_n$ tale che $[a][c] = [ac] = [1]$, ovvero $[a]$ è invertibile se, e solo se, esiste $c \in \mathbb{Z}$ tale che $ac \equiv 1 \pmod{n}$. Tale osservazione suggerisce l'introduzione della seguente definizione: se a e b sono interi, e $n \in \mathbb{N}^*$, si dice *soluzione* dell'*equazione congruenziale*

$$(*) \quad ax \equiv b \pmod{n}$$

ogni intero c tale che risulti

$$ac \equiv b \pmod{n}.$$

Ciò equivale a richiedere, ovviamente, che sia $[a][c]=[b]$. Secondo questa definizione, dunque, $[a] \in \mathbb{Z}_n$ è invertibile se, e solo se, l'equazione congruenziale

$$ax \equiv 1 \pmod{n}$$

ammette una soluzione c ; in tal caso risulterà $[c] = [a]^{-1}$.

Si fornirà ora una condizione necessaria e sufficiente affinché l'equazione congruenziale (*) ammetta soluzioni (ovvero, come si dice, sia *risolubile*), nonché un procedimento che permetta di determinare l'insieme delle soluzioni di (*), quando tali soluzioni esistano.

Proposizione 12 Siano a, b interi, $n \in \mathbb{N}^*$, $d = \text{M.C.D.}(a, n)$. L'equazione congruenziale (*)

$$ax \equiv b \pmod{n}$$

ha soluzione se, e solo se, d divide b .

Dim. Se c è una soluzione di (*), esiste $k \in \mathbb{Z}$ tale che $ac - b = kn$. Allora, da $d \mid a$ e $d \mid n$ segue $d \mid ac - kn = b$.

Viceversa, si supponga d divisore di b : esiste dunque $h \in \mathbb{Z}$ tale che $b = dh$. Essendo inoltre d un massimo comune divisore tra a ed n , esistono degli interi r ed s tali che $d = ra + sn$. Da ciò segue $b = hd = h(ra + sn) = hra + hsn$; in particolare, da $hra - b = -hsn$ segue che hr è una soluzione di (*).

Osservazione La prop.12 segue immediatamente anche dalla teoria delle equazioni diofantee.

Proposizione 13 Siano a, b interi, $n \in \mathbb{N}^*$, t un divisore comune di a , b , n . Allora le soluzioni dell'equazione congruenziale

$$ax \equiv b \pmod{n}$$

sono tutte e sole quelle dell'equazione congruenziale

$$\frac{a}{t}x \equiv \frac{b}{t} \pmod{\frac{n}{t}}.$$

Dim. E' sufficiente osservare che, se c è un intero, $n = t \frac{n}{t}$ divide $ac - b = t \frac{a}{t}c - t \frac{b}{t}$ se, e solo se, $\frac{n}{t}$ divide $\frac{a}{t}c - \frac{b}{t}$.

Proposizione 14 Sia c una soluzione dell'equazione congruenziale

$$ax \equiv 1 \pmod{n}.$$

Allora, se b è un intero, cb è soluzione dell'equazione congruenziale

$$ax \equiv b \pmod{n}.$$

Dim. Basta osservare che, se n divide $ac - 1$, divide anche $(ac - 1)b = acb - b$.

Proposizione 15 Si consideri l'equazione congruenziale

$$(*) \quad ax \equiv b \pmod{n},$$

e siano a ed n primi tra loro. Allora l'equazione $(*)$ ha soluzioni, che costituiscono una classe resto modulo n .

Dim. Poiché $1 = \text{M.C.D.}(a,n)$ divide b , per la prop.12 l'equazione $(*)$ ha soluzioni. Indicata con c una di tali soluzioni, verifichiamo che l'insieme X di tutte e sole le soluzioni di $(*)$ coincide con $[c]_n$. Sia $y \in X$; da $ac \equiv b \pmod{n}$ e $ay \equiv b \pmod{n}$ segue $ac \equiv ay \pmod{n}$, cioè $n \mid ac - ay = a(c-y)$; ciò implica, essendo inoltre n ed a primi tra loro, che n divide $c-y$, per cui $y \in [c]_n$. Viceversa, se $y \in [c]_n$, risulta $[c]_n = [y]_n$, e quindi $[a]_n [y]_n = [a]_n [c]_n = [b]_n$, come si voleva.

Un algoritmo per risolvere l'equazione congruenziale

$$(*) \quad ax \equiv b \pmod{n}.$$

Caso A : *risoluzione dell'equazione congruenziale del tipo:*

$$ax \equiv 1 \pmod{n}$$

con $\text{M.C.D.}(a,n) = 1$.

Essendo $1 = \text{M.C.D.}(a,n)$, è possibile determinare, mediante l'algoritmo di Euclide delle divisioni successive (vedi Appendice), degli interi α, β tali che risulti $\alpha a + \beta n = 1$; α risulta essere una soluzione dell'equazione e $[\alpha]_n$ (cfr. prop.15) coincide con l'insieme di tutte le soluzioni dell'equazione.

Caso B: *risoluzione della generica equazione congruenziale*

$$(*) \quad ax \equiv b \pmod{n}.$$

1) *Verificare che $d = \text{M.C.D.}(a,n)$ divida b .*

Infatti, per la prop.12, questa è condizione necessaria e sufficiente affinché l'equazione $(*)$ ammetta soluzioni. Se d divide b , passare al punto seguente:

2) Posto $\bar{a} = \frac{a}{d}$, $\bar{b} = \frac{b}{d}$, $\bar{n} = \frac{n}{d}$, *considerare l'equazione congruenziale*

$$(**) \quad \bar{a}x \equiv \bar{b} \pmod{\bar{n}},$$

che per la prop.13 ammette tutte e sole le soluzioni di $(*)$, ed è tale che $\text{M.C.D.}(\bar{a}, \bar{n}) = 1$;

3) *Determinare una soluzione c dell'equazione congruenziale*

$$(\diamond) \quad \bar{a}x \equiv 1 \pmod{\bar{n}}$$

mediante il metodo illustrato nel caso A; per la prop.14, $c\bar{b} = \bar{c}$ sarà soluzione di (**).

- 4) Per la prop.15, l'insieme X delle soluzioni di (**), e quindi di (*), coincide con la classe resto $[\bar{c}]_{\bar{n}}$.

Esempio Si dica se l'equazione congruenziale

$$20x \equiv 4 \pmod{34}$$

ammette soluzioni; in caso di risposta affermativa, determinare l'insieme di tutte le soluzioni.

Risoluzione

- 1) M.C.D.(20,34) = 2 divide 4. Allora l'equazione ammette soluzioni, che coincidono con quelle dell'equazione:

2) $10x \equiv 2 \pmod{17}$

- 3) si studia l'equazione:

$$10x \equiv 1 \pmod{17}$$

(vedi caso A): mediante l'algoritmo di Euclide (vedi esempio dell'Appendice) si determinano degli interi h e k tali che $1 = h10 + k17$; in questo caso, $h = -5$ e $k = +3$. Allora -5 è soluzione di

$$10x \equiv 1 \pmod{17}$$

e $(-5)2 = -10$ è soluzione di

$$10x \equiv 2 \pmod{17}.$$

- 4) L'insieme delle soluzioni dell'equazione

$$10x \equiv 2 \pmod{17}$$

coincide con la classe $[-10]_{17} = [7]_{17}$, ovvero è l'insieme $\{7 + k17 : k \in \mathbb{Z}\} = 7 + 17\mathbb{Z}$.

APPENDICE

In questa appendice si evidenzia come, se $d = \text{M.C.D.}(a,b)$, è possibile determinare, tramite l'*algoritmo di Euclide* (cfr. cap.1, 4.6), degli interi h e k tali che $d = ha + kb$. Supposto $b \neq 0$, con le notazioni di 4.6 risulta $r_n = d = \text{M.C.D.}(a,b)$, ed $r_s = r_{s-2} - r_{s-1}q_s$, per ogni s tale che $1 \leq s \leq n$.

Si procede allora per sostituzioni successive, partendo dall'uguaglianza

$$r_n = r_{n-2} - r_{n-1}q_n$$

e sostituendo ogni volta i resti r_s che figurano nell'uguaglianza con la differenza $r_{s-2} - r_{s-1}q_s$. Alla fine di questa sequenza di sostituzioni, r_n sarà espresso come somma di prodotti, in ognuno dei quali sarà presente il fattore $r_{-1} = a$ oppure $r_0 = b$, e basterà allora

mettere in evidenza a e b per ottenere l'espressione richiesta. Un esempio contribuirà a chiarire il procedimento sopra esposto:

Esempio Determinare degli interi h e k tali che $1 = M.C.D.(17,10) = k17+h10$.

Si determini $1 = M.C.D.(17,10)$ mediante l'algoritmo di Euclide, evidenziando eventualmente l'espressione $r_s = r_{s-2} - r_{s-1}q_s$:

$$17 = 10 \cdot 1 + 7 \quad ; \quad 7 = 17 - 10 \cdot 1$$

$$10 = 7 \cdot 1 + 3 \quad ; \quad 3 = 10 - 7 \cdot 1$$

$$7 = 3 \cdot 2 + 1 \quad ; \quad 1 = 7 - 3 \cdot 2$$

$$3 = 3 \cdot 1$$

Si consideri ora l'espressione

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

e si eseguano, a partire da questa, le sostituzioni indicate nel procedimento:

$$1 = 7 - 3 \cdot 2 = (*) \quad 7 - (10 - 7 \cdot 1) \cdot 2 = 7 - 10 \cdot 2 + 7 \cdot 2 = 7 \cdot 3 - 10 \cdot 2 = (**)(17 - 10 \cdot 1) \cdot 3 - 10 \cdot 2 = 17 \cdot 3 - 10 \cdot 3 - 10 \cdot 2 = 17(3) + 10(-3-2) = 3 \cdot 17 + (-5) \cdot 10.$$

(*) sostituisco 3

(**) sostituisco 7

Si sono così determinati $k = +3$ e $h = -5$