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

Per ogni $n \in \mathbb{Z}$, si consideri in $\mathbb{Z}$ la relazione così definita:

$$a \equiv_n b \Leftrightarrow n \text{ divide } a-b.$$

La relazione binaria $\equiv_n$ è detta ***congruenza modulo n***. Se $a \equiv_n b$ scriveremo pure $a \equiv b \pmod{n}$ e leggeremo ***a congruo b (modulo n)*.**

Esempio: $5 \equiv_7 19$, perché $7 \mid 5-19=-14$, mentre 4 non è nella relazione $\equiv_5$ con 8, perché 5 non divide $4-8=-4$.

Osservazione 1 Si noti che $x \equiv_0 y$ se, e solo se, $x = y$, mentre risulta $x \equiv_1 y$, per ogni coppia (x,y) di interi. Dunque, la relazione $\equiv_0$ è l'uguaglianza, mentre la relazione $\equiv_1$ coincide con la relazione totale. Infine, poiché $n \mid x-y$ se, e solo se, $-n \mid x-y$, la relazione $\equiv_n$ coincide con quella $\equiv_{-n}$, per cui non si perderà di generalità quando si considererà la relazione $\equiv_n$, con $n \geq 0$.

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

Proposizione 2 Siano $x, y \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Risulta allora:

$$x \equiv y \pmod{n} \Leftrightarrow \text{rest}(x,n) = \text{rest}(y,n).$$

Dim. Sia $x \equiv y \pmod{n}$, e siano $q, r = \text{rest}(y,n)$ il quoziente e il resto della divisione di y per n: risulta allora $x-y = nh$ (per un $h \in \mathbb{Z}$) e $y = nq+r$. Ne segue $x = nh+y = nh+nq+r = n(h+q)+r$, con $0 \leq r \leq |n| = n$: per l'unicità del quoziente e del resto, r coincide con rest(x,n). Viceversa, sia $\text{rest}(x,n) = \text{rest}(y,n) = r$; ne segue che esistono $h, k \in \mathbb{Z}$ tali che $x = hn+r$, $y = kn+r$. Allora $x-y = hn+r-kn-r = n(h-k)$, e $x \equiv y \pmod{n}$.

Corollario 3 La congruenza mod. n è una relazione di equivalenza in $\mathbb{Z}$.

Dim. L'asserto è ovvio se $n = 0$. Se $n \in \mathbb{N}^*$, basta osservare che la congruenza mod. n è la relazione di equivalenza associata all'applicazione $f: x \in \mathbb{Z} \rightarrow \text{rest}(x, n) \in \mathbb{N}$.

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 $\mathbb{Z}/\equiv_n = \{ [a]_n / a\in\mathbb{Z} \}$ 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 4 Siano $a \in\mathbb{Z}$, $n \in\mathbb{N}$. Allora $[a]_n = \{ a+nk : k \in\mathbb{Z} \}$. Inoltre, se $n \neq 0$, e r è il resto della divisione di a per n, $[a]_n = [r]_n = \{x \in\mathbb{Z} : rest(x,n) = rest(a,n) = r \}$.

Dim Sussistono le seguenti uguaglianze: $[a]_n = \{ x\in\mathbb{Z} : x \equiv_n a\} = \{ x\in\mathbb{Z} :$ n divide x-a$\} = \{ x\in\mathbb{Z} : \exists k\in\mathbb{Z}$ tale che x-a = nk$\}=\{ x\in\mathbb{Z} : \exists k\in\mathbb{Z}$ tale che x = a+nk$\}=\{ a+nk : k \in\mathbb{Z} \}$.
Se poi è $n \neq 0$, sia a = nq+r, con $0 \leq r < |n| = n$. n divide a – r =nq, dunque $a \equiv_n r$ e $[a]_n = [r]_n$.
Per la prop. 2 si ha poi $[a]_n = \{ x\in\mathbb{Z} : x \equiv_n a\} = \{x \in\mathbb{Z} : rest(x,n) = rest(a,n) = r \}$.

Osservazione 5 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, l'insieme $\{ a+nk : k \in\mathbb{Z} \}$si indica con il simbolo $a+ n\mathbb{Z}$. La prop. 2 si può riformulare dicendo che $[a]_n = a+ n\mathbb{Z}$, per ogni $a,n\in\mathbb{Z}$.

Teorema 6 Se $n \geq 1$ è un intero, risulta $\mathbb{Z} /\equiv_n = \{[0], [1], [2], \ldots, [n-1]\}$, e gli elementi [0], [1], [2], …, [n-1] di $\mathbb{Z} /\equiv_n$ sono a due a due distinti. In particolare $\mathbb{Z} /\equiv_n$ ha ordine n.

Dim. Dalla prop. 4 segue che, se $a\in\mathbb{Z}$, [a] = [rest(a,n)]. Da $0 \leq rest(a,n) \leq n-1$ si deduce facilmente che $\mathbb{Z} /\equiv_n = \{ [a] / a\in\mathbb{Z} \} = \{[0], [1], [2], \ldots, [n-1]\}$.
Osserviamo poi esplicitamente che, se $r \in\{0, 1,\ldots, n-1\}$, risulta $r = 0\cdot n+r$, con $0 \leq r < |n| = n$, e quindi r = rest(r,n). Ne segue allora che gli elementi [0], [1], [2], …, [n-1] di $\mathbb{Z} /\equiv_n$ sono a due a due distinti, risultando $r = rest(r,n) \neq rest(s,n) = s$, se $0 \leq r < s \leq n-1$.

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 $(\mathbb{Z}_n,+,\bullet)$

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 $[a], [b] \in\mathbb{Z}_n$

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

$$[a]\cdot[b] = [ab]$$

La struttura quoziente $(\mathbb{Z}_n,+,\bullet)$ risulta essere, al pari di $(\mathbb{Z},+,\bullet)$, un anello commutativo unitario, che è detto l'***anello delle classi resto modulo n*** (cfr.cap.4, §24, §27). Non tutte le proprietà di $(\mathbb{Z},+,\bullet)$ sono però ereditate da $(\mathbb{Z}_n,+,\bullet)$: 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 $(\mathbb{Z}_n,+,\bullet)$.

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 = 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 $\alpha a \equiv 1$ (mod.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 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 = 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 iii), si osservi che, se n è primo, tutti gli interi 1, 2, …, n-1 sono primi con n, e quindi tutte le classi [1], [2],…, [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 M.C.D.$(n_1,n) = n_1 > 1$. Dall'assurdo segue che n è necessariamente primo.

Esempio Gli anelli $\mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_{11}$ 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***

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

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 affinchè 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=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

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

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

Dim. Poiché 1 = 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

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

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

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

con M.C.D.(a,n) = 1.

Essendo 1 = 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*

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

1) *Verificare che d = M.C.D.(a,n) divida b.*

Infatti, per la prop.12, questa è condizione necessaria e sufficiente affinchè 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*

(**) $\bar{a}\,x \equiv \bar{b}$ *(mod.* $\bar{n}$*),*

che per la prop.13 ammette tutte e sole le soluzioni di (*), ed è tale che

M.C.D.$(\bar{a}, \bar{n}) = 1$;

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

(◊) $\bar{a}\,x \equiv 1$ *(mod.* $\bar{n}$*)*

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

$$20x \equiv 4 \text{ (mod.34)}$$

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) $$10x \equiv 2 \text{ (mod.17)}$$

3) si studia l'equazione:

$$10x \equiv 1 \text{ (mod.17)}$$

(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

$$10x \equiv 1 \text{ (mod.17)}$$

e (-5)2 = -10 è soluzione di

$$10x \equiv 2 \text{ (mod.17).}$$

4) L'insieme delle soluzioni dell'equazione

$$10x \equiv 2 \text{ (mod.17)}$$

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 = 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 $r_n = d = M.C.D.(a,b)$, 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 $r_s = r_{s-2} – r_{s-1}q_s$:

$17 = 10\cdot1+7$; $7 = 17-10\cdot1$

$10 = 7\cdot1+3$; $3 = 10-7\cdot1$

$7 = 3\cdot2+1$; $1 = 7- 3\cdot2$

$3 = 3\cdot1$

Si consideri ora l'espressione

$1 = 7- 3\cdot2$

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

$1 = 7- 3\cdot2$ = (*) $7 –(10-7\cdot1)\cdot2 = 7 -10\cdot2+7\cdot2 = 7\cdot3 -10\cdot2$ = (**)$(17-10\cdot1)\cdot3 - 10\cdot2= 17\cdot3 -10\cdot3-10\cdot2= 17(3)+10(-3-2) = 3\cdot17+(-5)\cdot10$.

(*) sostituisco 3

(**) sostituisco 7

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