Aritmetica modulare

Mauro Saita
e-mail: maurosaita@tiscalinet.it

Versione provvisoria. Febbraio 2018.[1]

Indice

[1] Nome File: aritmetica_modulare_2018.tex

1 Aritmetica modulare. Classe di resti

Cominciamo con un esempio.

Consideriamo la seguente tabella ottenuta eseguendo, per ogni numero intero, la divisione per quattro.

$\mathbb{Z}$	divisione per 4	quoziente	resto
⋮	⋮	⋮	⋮
-4	-4:4	-1	0
-3	-3:4	-1	1
-2	-2:4	-1	2
-1	-1:4	-1	3
0	0:4	0	0
1	1:4	0	1
2	2:4	0	2
3	3:4	0	3
4	4:4	1	0
⋮	⋮	⋮	⋮

Come già sapevamo tutti i possibili resti sono rappresentati dai numeri 0,1,2,3.

Costruiamo allora un'altra tabella avente una colonna per ogni possibile resto e poniamo in ognuna di esse tutti i numeri interi che, divisi per quattro, danno il resto corrispondente alla colonna in esame.

Quindi, poniamo in $r = 0$ tutti i numeri interi che divisi per quattro danno resto zero, in $r = 1$ tutti i numeri interi che divisi per quattro danno resto uno e così via.

$r = 0$	$r = 1$	$r = 2$	$r = 3$
⋮	⋮	⋮	⋮
-12	-11	-10	-9
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
⋮	⋮	⋮	⋮

In questo modo otteniamo una *partizione* dell'insieme $\mathbb{Z}$ in *quattro classi*, una per ogni colonna della precedente tabella.

Poniamoci ora la seguente domanda.

Dati due qualsiasi numeri interi x e y come possiamo stabilire se appartengono o meno alla stessa classe?

La risposta è semplice: occorre dividere i due numeri x e y per quattro e verificare se hanno lo stesso resto. In caso affermativo i due numeri prescelti appartengono alla stessa classe, altrimenti no.

Riflettiamo un poco su ciò che abbiamo appena imparato: la costruzione delle due precedenti tabelle e la successiva partizione dell'insieme $\mathbb{Z}$ sono state possibili perché, all'inizio di questo paragrafo, abbiamo scelto di dividere tutti gli interi per il numero $n = 4$.

In realtà questa scelta non era obbligata; per esempio, se avessimo diviso tutti gli interi per $n = 7$ avremmo ancora ottenuto una partizione di $\mathbb{Z}$ in classi, quelle corrispondenti a tutti i possibili resti della divisione per sette e cioè 0, 1, 2, 3, 4, 5, 6.

Insomma, tutto ciò che abbiamo fin qui esposto ed in particolare, la partizione di $\mathbb{Z}$ in classi di equivalenza è realizzabile scegliendo un qualunque intero $n > 0$; ovviamente quello che cambia sono le classi!.

Queste considerazioni ci inducono a dare la seguente importante

Definizione 1.1. *Dati due numeri x e y appartenenti a $\mathbb{Z}$ ed un intero $n > 0$ diciamo che "x è congruo a y modulo n e scriviamo*

$$x \equiv y \qquad (mod\, n)$$

se e solo se x e y divisi per n danno lo stesso resto.

La relazione di congruenza che abbiamo appena introdotto[2] suddivide l'insieme $\mathbb{Z}$ dei numeri interi in n classi che chiamiamo *classi di resti modulo n*. Scriveremo così:

$$[0], [1], [2], \ldots, [n-1]$$

Indichiamo inoltre con $\mathbb{Z}_n$ l'insieme costituito da queste classi di resti e cioè:

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

Esercizio 1.2. *Determinare le classi che si ottengono dalle seguenti congruenze:*

$$\begin{array}{llll} a] & x \equiv y & (mod\, 4); & \qquad c] \quad x \equiv y \quad (mod\, 8); \\ b] & x \equiv y & (mod\, 5); & \qquad d] \quad x \equiv y \quad (mod\, 12). \end{array}$$

Esercizio 1.3. *Nell'insieme $\mathbb{Z}$ dei numeri interi verificare se sono vere o false le seguenti congruenze, giustificando le risposte.*

$$\begin{array}{llll} a] & 10 \equiv 13 & (mod\, 3); & \qquad d] \quad 100 \equiv 1 \quad (mod\, 9); \\ b] & 2 \equiv 8 & (mod\, 5); & \qquad e] \quad 25 \equiv 5 \quad (mod\, 3); \\ c] & 20 \equiv 4 & (mod\, 6); & \qquad f] \quad 17 \equiv 5 \quad (mod\, 4). \end{array}$$

[2]Si può dimostrare che la definizione 1.1 è equivalente alla seguente: "se a e b sono interi, diciamo che x è *congruo a y modulo n*, e scriviamo $x \equiv y \pmod{n}$ (o anche $x \equiv_n y$) se e solo se la differenza $x - y$ è un multiplo di n."

1.1 Le proprietà delle congruenze

Per una "congruenza" valgono le seguenti proprietà.

1. Per ogni $x \in \mathbb{Z}$, $\quad x \equiv x \pmod{n}$ (proprietà riflessiva)

2. Per ogni $x, y \in \mathbb{Z}$,
se $x \equiv y \pmod{n}$ allora $\quad y \equiv x \pmod{n}$ (proprietà simmetrica)

3. Per ogni $x, y, z \in \mathbb{Z}$,
se $x \equiv y \pmod{n}$ e $\quad y \equiv z \pmod{n}$
allora $\quad x \equiv z \pmod{n}$ (proprietà transitiva)

Esercizio 1.4. *Dimostrare le precedenti proprietà argomentando in modo chiaro e dettagliato.*

1.2 Le operazioni in $\mathbb{Z}_n$: l'addizione e la moltiplicazione

In quale modo si possono sommare gli elementi di $\mathbb{Z}_5$? E in quale modo si possono moltiplicare?

Procediamo così:

$$[0]+[1]=[0+1]=[1] \qquad [0]\cdot[1]=[0\cdot 1]=[0]$$
$$[0]+[2]=[0+2]=[2] \qquad [0]\cdot[2]=[0\cdot 2]=[0]$$
$$[0]+[3]=[0+3]=[3] \qquad [0]\cdot[3]=[0\cdot 3]=[0]$$
$$\ldots\ \ldots\ \ldots \qquad \ldots\ \ldots\ \ldots$$
$$[1]+[1]=[1+1]=[2] \qquad [1]\cdot[1]=[1\cdot 1]=[1]$$
$$\ldots\ \ldots\ \ldots \qquad \ldots\ \ldots\ \ldots$$
$$[2]+[4]=[2+4]=[6]=[1] \qquad [2]\cdot[4]=[2\cdot 4]=[8]=[3]$$

Questo ultimo caso è un poco diverso dagli altri; infatti, essendo $6 = 5 \cdot 1 + 1$, abbiamo $[6] = [1]$. Analogamente $8 = 5 \cdot 1 + 3$ e quindi $[8] = [3]$.

A questo punto siamo in grado di costruire la tabella della somma e quella del prodotto in $\mathbb{Z}_5$:

$+$	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

$\cdot$	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

In generale definiamo l'addizione e la moltiplicazione in Z_n nel seguente modo:

Definizione 1.5. *Se* $[a]$ *e* $[b]$ *sono due classi di resti modulo* n*, poniamo*

$$[a] + [b] = [a + b] \qquad e \qquad [a] \cdot [b] = [a \cdot b]$$

In questa definizione $[a]$ e $[b]$ sono classi di equivalenza individuate da un rappresentante (a e b rispettivamente); perché la nostra definizione sia sensata dobbiamo verificare che *il risultato della somma non dipende dal particolare rappresentante che abbiamo scelto per le due classi di resti che fanno da addendi (o da fattori).* In altre parole occorre verificare che

se $a' \equiv a$ e $b' \equiv b$ allora $a' + b' \equiv a + b$ e $a' \cdot b' \equiv a \cdot b$

Per non complicare troppo la nostra trattazione omettiamo, per il momento, queste verifiche.

Il problema che ora ci poniamo è il seguente: *dovendo eseguire dei calcoli in* $\mathbb{Z}_n$*, possiamo utilizzare tutte quelle proprietà algebriche che contraddistinguono gli ordinari insiemi numerici?* In altre parole, *quali proprietà caratterizzano la somma e il prodotto in* $\mathbb{Z}_n$*?*

Cominciamo allora ad occuparci dell'addizione.

In $\mathbb{Z}_n$ valgono le seguenti importanti proprietà

1. Proprietà commutativa:
   per ogni $[a], [b] \in \mathbb{Z}_n$ $\qquad [a] + [b] = [b] + [a]$
2. Proprietà associativa:
   per ogni $[a], [b], [c] \in \mathbb{Z}_n$ $\qquad ([a] + [b]) + [c] = [a] + ([b] + [c])$
3. Esistenza dell'elemento neutro:
   per ogni $[a] \in \mathbb{Z}_n$ abbiamo $[a] + [0] = [0] + [a] = [a]$
   Questo significa che la classe individuata dal numero zero non produce alcun effetto se sommata ad una qualsiasi altra classe.Per questa ragione chiamiamo la classe $[0]$ *elemento neutro rispetto alla somma.*
4. Esistenza dell'inverso rispetto alla somma:
   per ogni elemento $[a] \in \mathbb{Z}_n$ esiste un elemento che denotiamo con $[-a]$, detto *inverso di* $[a]$ *rispetto alla somma* o più semplicemente *opposto di* $[a]$, per il quale
   $$[a] + [-a] = [-a] + [a] = [0]$$

Le proprietà sopra esposte ci consentono di affermare che l'insieme $\mathbb{Z}_n$ è un *gruppo commutativo* (o anche *gruppo abeliano* [3]) rispetto alla somma.

[3] Dal nome del matematico norvegese N. H. Abel (1802-1829).

Dobbiamo però fare attenzione , perchè la somma in $\mathbb{Z}_n$ può riservare qualche sorpresa. Per esempio, in $\mathbb{Z}_4$ abbiamo:

$$[2] + [2] = [0]$$

Quindi, il luogo comune secondo il quale *in matematica, due più due fa sempre quattro* risulta, in questo caso, palesemente falso!

Esercizio 1.6. *Eseguire le seguenti somme mod n:*

a)	$4+3=$	$\ldots\ldots$ $(mod\,3)$;	*d*)	$2+5=$	$\ldots\ldots$ $(mod\,2)$;
b)	$4+3=$	$\ldots\ldots$ $(mod\,4)$;	*e*)	$2+5=$	$\ldots\ldots$ $(mod\,3)$;
c)	$4+3=$	$\ldots\ldots$ $(mod\,5)$;	*f*)	$2+5=$	$\ldots\ldots$ $(mod\,6)$;

Esercizio 1.7. *Verificare che $\mathbb{Z}_4$ è un gruppo abeliano rispetto alla somma. (Costruire la tabella relativa alla somma in $\mathbb{Z}_4$ e poi verificare le quattro proprietà sopra enunciate).*

Per quanto rigurda il *prodotto* sussistono invece le seguenti proprietà:

1. Proprietà commutativa:
   per ogni $[a], [b] \in \mathbb{Z}_n$ $\qquad [a] \cdot [b] = [b] \cdot [a]$
2. (Proprietà associativa:
   per ogni $[a], [b], [c] \in \mathbb{Z}_n$ $\qquad ([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$
3. Esistenza dell'elemento neutro:
   per ogni $[a] \in \mathbb{Z}_n$ abbiamo
   $$[a] \cdot [1] = [1] \cdot [a] = [a]$$
   Questo significa che la classe individuata dal numero uno non produce alcun effetto se moltiplicata per una qualsiasi altra classe. Per questa ragione chiamiamo la classe [1] *elemento neutro rispetto al prodotto.*

1.3 Elementi invertibili nelle classi di resto.

Come avrete notato non abbiamo incluso tra le proprietà del prodotto quella relativa all'esistenza dell'inverso. Infatti, in certe classi di resti, non tutti gli elementi ammettono inverso rispetto al prodotto. Per esempio, dalla tabella relativa alla moltiplicazione in $\mathbb{Z}_6$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

ci accorgiamo subito che le classi [2], [3] e [4] non hanno inverso.

In generale, vale infatti il seguente

Teorema 1.8. *Un elemento $a \in \mathbb{Z}_n$ è invertibile se e solo se a è primo con n, cioè se e solo se $MCD(a, n) = 1$. In particolare, se p è un numero primo, allora ogni elemento non nullo di $\mathbb{Z}_p$ è invertibile.*

Dimostrazione. Supponiamo che $[a] \in \mathbb{Z}_n$ sia invertibile, vale a dire supponiamo che esista una classe $[b]$ in $\mathbb{Z}_n$ per la quale $[a] \cdot [b] = 1$ in $\mathbb{Z}_n$. Questo significa che, in $\mathbb{Z}$, $ab - 1 = hn$ per qualche intero h, ovvero che

$$ab - hn = 1.$$

Da quest'ultima uguaglianza segue che ogni intero che divide sia a che n deve dividere anche 1, e quindi il massimo comun divisore di a e n è 1.

Viceversa, se a e n sono primi tra loro, allora esistono interi x, y per i quali $ax + ny = 1$. (Si veda **??**). Allora $ax = 1$ in $\mathbb{Z}_n$, ovvero a è invertibile in $\mathbb{Z}_n$, con inverso x. □

Osservazione

Ricordiamo la definizione della funzione φ di Eulero: per ogni intero m, $\varphi(m)$ è il numero degli interi t, $1 \leq t \leq m$, che sono primi con m. Dunque, per il teorema precedente, *il numero degli elementi invertibili di $\mathbb{Z}_m$ è $\varphi(m)$.*

Esercizio 1.9. *Eseguire le seguenti moltiplicazioni mod n:*

a)	$4 \cdot 3 =$	$\ldots\ldots$ $(mod\,3)$;	*d)*	$2 \cdot 5 =$	$\ldots\ldots$ $(mod\,2)$;
b)	$4 \cdot 3 =$	$\ldots\ldots$ $(mod\,4)$;	*e)*	$2 \cdot 5 =$	$\ldots\ldots$ $(mod\,3)$;
c)	$4 \cdot 3 =$	$\ldots\ldots$ $(mod\,5)$;	*f)*	$2 \cdot 5 =$	$\ldots\ldots$ $(mod\,6)$;

Esercizio 1.10. *Determinare gli inversi di tutti gli elementi di $\mathbb{Z}_5$ diversi da [0].*

Esercizio 1.11. *Stabilire se la seguente affermazione è vera o falsa e motivare la risposta: "in Z_n vale la legge di annullamento del prodotto" e cioè*

$$per \quad ogni \quad [a], [b] \in \mathbb{Z}_n \quad se \quad [a] \cdot [b] = [0] \quad allora \quad [a] = [0] \quad oppure \quad [b] = [0].$$

Soluzione. L'affermazione è falsa infatti in $\mathbb{Z}_n$, *esistono classi diverse da zero il cui prodotto è la classe zero.* Per esempio in $\mathbb{Z}_6$ abbiamo $[2] \cdot [3] = [0]$ ed anche $[3] \cdot [4] = [0]$.

Esercizio 1.12. *Stabilire se la seguente affermazione è vera o falsa e motivare la risposta: "in $\mathbb{Z}_n$ vale la legge di cancellazione del prodotto" e cioè*

$$per \quad ogni \quad [a], [b], [c] \in \mathbb{Z}_n \quad se \quad [a] \cdot [c] = [b] \cdot [c] \quad allora \quad [a] = [b].$$

Esercizio 1.13. *Verificare che il polinomio $p(x) = x^4 - 117x + 39$ non ammette radici intere.*

Esercizio 1.14. *Servendosi di un foglio elettronico, determinare le seguenti classi di resti: $\mathbb{Z}_2$, $\mathbb{Z}_6$ e $\mathbb{Z}_{11}$.*

Esercizio 1.15. *Utilizzando Excel, costruire la tavola della moltipilicazione per le classi di resto mod(26). Individuare gli elementi invertibili e per ognuno di essi determinare l'inverso.*