

Aritmetica modulare

Consideriamo tutti i numeri interi relativi \mathbf{Z} , e su questo insieme definiamo una relazione di equivalenza come segue:

fissato un numero intero n , diremo che due numeri a e b sono congrui modulo n se:

$$a = b + kn, k \in \mathbf{Z}.$$

Se è verificata la relazione sopra riportata scriveremo anche che $a \equiv b \pmod{n}$ (che si legge *a congruo a b modulo n*).

Verifichiamo che quella scritta è effettivamente una relazione di equivalenza. Infatti per tale relazione valgono le seguenti proprietà:

- **riflessiva:** $a \equiv a \pmod{n}$. Infatti comunque si scelga il numero intero a risulta $a - a = 0 \cdot n$.
- **simmetrica:** se $a \equiv b \pmod{n}$ allora vale anche $b \equiv a \pmod{n}$. Se $a \equiv b \pmod{n}$ esiste un numero intero relativo k tale che: $a - b = kn$. È immediato verificare che risulta anche: $b - a = -kn$, dato che $-k \in \mathbf{Z}$ allora risulta anche $b \equiv a \pmod{n}$.
- **transitiva:** se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, allora $a \equiv c \pmod{n}$. Se $a \equiv b \pmod{n}$ deve esistere un numero intero relativo k_1 tale che: $a - b = k_1n$; in modo analogo se $b \equiv c \pmod{n}$, deve esistere un numero intero relativo k_2 che soddisfi la relazione: $b - c = k_2n$. Sommando le due uguaglianze prima scritte otteniamo: $a - c = (k_1 + k_2)n$, che ci permette di concludere che anche $a \equiv c \pmod{n}$.

La relazione scritta quindi è una relazione di equivalenza, possiamo quindi suddividere l'insieme \mathbf{Z} in classi di equivalenza. Per rappresentare tali classi, che sono esattamente n , possiamo utilizzare i seguenti simboli, già utilizzati da Gauss:

$$[0], [1], [2], \dots, [n-1].$$

L'elemento scritto tra parentesi quadre viene detto *rappresentante* della classe di resto modulo n , tale numero è uno qualsiasi dei numeri appartenenti alla classe di resto scelta. Normalmente si utilizza quale rappresentante il numero intero positivo compreso tra 0 e $n-1$ che appartiene alla classe di resto.

Notiamo un fatto che risulterà utile nel seguito: fissato un intero n , due numeri interi a e b appartengono alla stessa classe di resto modulo n se hanno lo stesso resto nella divisione per n . Infatti ammettiamo che $a, b \equiv [c] \pmod{n}$. Ciò significa che: devono esistere due numeri interi $k_1, k_2 \in \mathbf{Z}$, tali che risulti $a = c + k_1n$ e $b = c + k_2n$. Tra tutti i possibili valori di c , rappresentante della classe alla quale appartengono i due numeri assegnati, possiamo scegliere quello che soddisfa la condizione: $0 \leq c < n$; quindi, utilizzando la definizione di quoziente e resto della divisione di numeri interi possiamo anche concludere che i due numeri, divisi per n hanno quale resto il valore comune c .

L'insieme delle classi di equivalenza prima definite viene normalmente indicato con il simbolo \mathbf{Z}_n e viene normalmente indicato come insieme delle classi di resto modulo n .

Su questi particolari insiemi finiti possiamo definire alcune due operazioni:

- **somma di classi di resto modulo n .** Fissato n ed assegnate due classi di resto modulo n , siano $[a]$ e $[b]$, definiamo la somma nel seguente modo:

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

Esempio: in \mathbf{Z}_5 , insieme delle classi di resto modulo 5, date le classi $[3]$ e $[4]$, definiamo: $[3] + [4] = [7]$. La classe $[7]$ in \mathbf{Z}_5 coincide con la classe $[2]$, quindi normalmente scriveremo che $[3] + [4] = [2]$ in \mathbf{Z}_5 .

Prima di procedere dobbiamo verificare che la definizione è **ben posta**. Ovvero dobbiamo dimostrare che il risultato dell'operazione non dipende dal particolare rappresentate scelto.

Fissato un numero intero n , siano $[a]$ e $[b]$ due classi di resti modulo n e siano a', b' due rappresentanti per le stesse classi, ovvero: $[a] = [a']$ e $[b] = [b']$. Verifichiamo che risulta anche: $[a] + [b] = [a'] + [b']$, $[a + b] = [a' + b']$. Se a e a' appartengono alla stessa classe di resto modulo n deve risultare: $a - a' = k_1 n$, per un opportuno valore di $k_1 \in \mathbf{Z}$. In modo analogo deve risultare: $b - b' = k_2 n$, con k_2 opportuno. Possiamo anche scrivere che: $a = a' + k_1 n$ e $b = b' + k_2 n$, sommando ambi i membri delle due uguaglianze precedenti risulta: $a + b = a' + b' + (k_1 + k_2)n$ e questo ci permette di concludere che $a + b$ e $a' + b'$ appartengono alla stessa classe di resti modulo n , e finalmente possiamo concludere che $[a + b] = [a] + [b] = [a'] + [b'] = [a' + b']$. Quindi il risultato dell'operazione prima definita non dipende dal rappresentante scelto, ma dipende esclusivamente dalle classi che vengono sommate.

Per l'operazione prima definita valgono le seguenti proprietà:

1. la legge di composizione è interna;
 2. è associativa;
 3. è commutativa;
 4. esiste un elemento particolare detto neutro (la classe $[0]$, ovvero la classe formata da tutti i multipli interi relativi di n), che soddisfa la condizione: $[a] + [0] = [0] + [a] = [a]$.)
 5. per ogni classe di resto esiste l'elemento inverso nell'operazione di somma, (data una classe di resto, sia $[a]$, esiste un'altra classe di resto, la classe $[-a]$, tale che $[a] + [-a] = [-a] + [a] = [0]$).
- **prodotto di classi di resto modulo n .** Analogamente a quanto fatto in precedenza definiamo il prodotto di due classi di resto nel seguente modo:

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

Esempio. In \mathbf{Z}_6 il prodotto di $[2]$ per la classe $[3]$ è la classe $[6] = [0]$.

Anche in questo caso possiamo verificare che il prodotto di due classi di resto modulo n non dipende dalla scelta del rappresentante, quindi anche questa definizione è ben posta.

Le proprietà che valgono per questa operazione sono le seguenti:

1. la legge di composizione è interna;
2. vale la proprietà associativa;
3. vale la proprietà commutativa;
4. esiste l'elemento neutro (la classe $[1]$ moltiplicata per una qualsiasi altra classe $[a]$, dà quale risultato la classe $[a]$);
5. se p è un numero primo tutte le classi di \mathbf{Z}_p , esclusa la classe $[0]$, hanno inverso in questa operazione (data una classe in \mathbf{Z}_p diversa dalla classe $[0]$, esiste sempre una classe, sia $[a']$ tale che risulti: $[a] \cdot [a'] = [1]$).

Utilizzando quanto detto prima è possibile mostrare che nell'insieme delle classi di resto modulo n valgono le seguenti uguaglianze:

$$[a + b] = [a] + [b], [a \cdot b] = [a] \cdot [b].$$

Queste semplici considerazioni ci permettono di illustrare come si possono ottenere i noti criteri di divisibilità.

Divisibilità per 2. Questo criterio non richiede una dimostrazione, però permette di introdurre un metodo di procedere che risulterà particolarmente utile nel seguito.

Sia N un numero intero, N può essere scritto nel seguente modo, in base 10, $N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10 + a_0$, con $a_n \neq 0$ e $a_j, j = 1, \dots, n-1$ cifra compresa tra 0 e 9.

Il numero N è divisibile per 2 se le classi di resto modulo 2 $[N]$ e $[0]$ coincidono.

Utilizzando quanto scritto in precedenza possiamo dire che in \mathbf{Z}_2 vale:

$$[N] = [a_n] \cdot [10^n] + [a_{n-1}] \cdot [10^{n-1}] + \dots + [a_1] \cdot [10] + [a_0] = [a_0],$$

in quanto in \mathbf{Z}_2 $[10^k] = [0]$. Un numero N è quindi divisibile per 2 se la cifra delle unità della scrittura di N in base 10 è divisibile per 2, quindi pari.

Divisibilità per 3. Utilizzando un procedimento analogo al precedente possiamo dire che un numero N è divisibile per 3 se in \mathbf{Z}_3 risulta $[N] = [0]$.

Per facilitare i calcoli iniziamo a notare che $[10] = [1]$ in \mathbf{Z}_3 ; da questo possiamo anche dedurre che $[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$. Ripetendo tale procedimento possiamo anche dire che $[10^k] = [1]$ per ogni intero positivo k .

Utilizzando la scrittura in base 10 del numero intero N risulta quindi:

$$[N] = [a_n] + [a_{n-1}] + \dots + [a_1] + [a_0] = [a_n + a_{n-1} + \dots + a_1 + a_0],$$

Quindi possiamo dire che il numero N è divisibile per 3 se risulta divisibile per 3 il numero ottenuto sommando le cifre che compongono il numero N nella sua scrittura decimale.

Divisibilità per 5. Operando come fatto in precedenza possiamo dire che in \mathbf{Z}_5 $[N] = [a_0]$ e tale classe coincide con la classe $[0]$ se a_0 è 0 oppure 5.

Divisibilità per 9. In questo caso $[10^k] = [1]$, come per il criterio di divisibilità per 3, abbiamo che il numero N è divisibile per 9 se la somma delle cifre del numero N scritto in base 10 sono divisibili per 9.

Divisibilità per 11. Iniziamo con il notare che $[10] = [-1]$ in \mathbf{Z}_{11} e che $[10^2] = [1]$, operando in tale modo possiamo dire che $[10^{2k}] = [1]$, mentre $[10^{2k+1}] = [-1]$, con $k \in \mathbf{N}$.

Possiamo quindi dire che:

$$[N] = [(-1)^n a_n] + [(-1)^{n-1} a_{n-1}] + \cdots + [-a_1] + [a_0].$$

Tale somma può essere riletta nel seguente modo:

un numero è divisibile per 11 se la somma delle cifre di posto pari diminuite delle cifre di posto dispari, è 0 oppure è divisibile per 11.

Il procedimento illustrato può essere utile per costruire anche altri criteri di divisibilità, ad esempio per 7, per 13, per 17 e così via, ma è possibile anche verificare che tali criteri risultano particolarmente laboriosi.

Per concludere un esercizio, tratto dalle prove di selezione delle olimpiadi italiane di matematica:

Esercizio. Sia $ABCDEF$ un numero intero di sei cifre che risulta divisibile per 7, dimostrare che è divisibile per 7 anche il numero $BCDEFA$.