Aritmetica Modulare

Andrea Canale

December 14, 2024

Contents

1 Congruenza

Dato un numero $N \geq 2$, chiamato modulo, e due numeri $m, n \in \mathbb{Z}$, questi numeri si dicono congruenti a modulo N se:

$$N \mid m - n$$

E lo scriviamo come

$$m \equiv n \; mod \; N$$

Notiamo che la congruenza è una relazione di equivalenza

2 Classi di equivalenza

Una classe di equivalenza su un numero è definita come segue:

$$[a]_N = \{b \in \mathbb{Z} | a \equiv b \ mod \ N\}$$

Alternativamente, se viene esplicitato il modulo si può scrivere come: $\overline{a}$

Questo tipo di classe si dice classe di resto, per calcolarle più facilmente si può scrivere:

$$[a]_N = \{a + kN \mid k \in \mathbb{Z}\} = a + N\mathbb{Z}$$

Notiamo che le classi di resto hanno una certa ciclicità, ad esempio se $N = 5$, sappiamo che $[5]_5 = [0]_5$ e così via.

Inoltre le classi di resto di N sono esattamente N

2.1 Rappresentante canonico

Sia $[a]_N$ una classe d'equivalenza, allora $[a]_N = [r]_N$ dove r è il resto della divisione $a : N$. Questa classe d'equivalenza viene detta rappresentante canonico.

3 Insieme delle classi di resto $\mathbb{Z}_\mathbb{N}$

L'insieme di tutte le classi di resto di un determinato modulo viene denotato come:

$$\mathbb{Z}_N = \{[0]_N, ..., [N-1]_N\}$$

Tutte le classi di resto formano un ricoprimento di $\mathbb{Z}$

3.1 Operazioni su $\mathbb{Z}_\mathbb{N}$

3.1.1 Addizione

L'addizione tra classi di resto viene definita come: $\overline{a} + \overline{b} = \overline{a+b}$

Inoltre valgono l'associatività e la commutatività.

L'elemento neutro è $\overline{0}$. L'inverso è $\overline{-a}$

3.1.2 Moltiplicazione

La moltiplicazione tra classi di resti è definita come: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Valgono l'associatività, la commutatività e la distributività.

La moltiplicazione ha come elemento neutro $\overline{1}$. L'esistenza dell'inverso non è garantita.

4 Invertibilità di classi

L'insieme delle classi invertibili è definito come

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n | \exists \overline{b} \in \mathbb{Z}_n \text{ t.c } \overline{a} \cdot \overline{b} = \overline{1}\}$$

La cardinalità di questo insieme è definita dalla funzione di Eulero. Tuttavia questa funzione non ha un andamento prevedibile.

4.1 Calcolare l'invertibilità di una classe

$[a]_N$ è invertibile se e solo se a è coprimo con il modulo.

4.2 Calcolare il valore della funzione di Eulero

Per i numeri primi, la funzione di Eulero si calcola come:

$$\varphi(p) = p - 1$$

Oppure per le potenze di numeri primi:

$$\varphi(p^n) = p^{n-1}(p-1)$$

Da ciò ne ricaviamo che per calcolare la funzione di Eulero per un generico numero n, dobbiamo prima scomporre in fattori primi e poi usare queste due formule per calcolare il risultato, moltiplicando tra loro i valori delle funzioni di Eulero per le singole funzioni.

Notiamo inoltre che se $MCD(a, b) = 1$, allora

$$\varphi(ab) = \varphi(a)\varphi(b)$$

5 Zero divisori

Una zero divisori in $\mathbb{Z}_N$ è una classe $\overline{a} \neq \overline{0}$ tale che $\overline{a} \cdot \overline{b} = \overline{0}$ per qualche $\overline{b} \neq \overline{0}$

$a \in \mathbb{Z}_N$ è uno zero divisore se e solo se $(a, N) > 1$

6 Generatori

Una classe ne genera un'altra se il modulo e il fattore sono coprimi.

7 Congruenze lineare

Una congruenza lineare è un'equivazione della forma $aX \equiv c \ mod \ N$ dove x è l'incognita che vogliamo risolvere.

Una congruenza di questo tipo è risolvibile se e solo se $d = MCD(a, N)$ divide c.

Abbiamo due casi:

- $MCD(a, N) = 1$, in questo caso sappiamo che esiste una soluzione
- $MCD(a, N) = d$, sappiamo che esistono d soluzioni in $mod \ N$

7.1 Trovare le soluzioni

Per trovare le soluzioni dobbiamo trovare l'identità di Bezout per (a,N) e il risultato sarà il coefficiente diverso da N