Introduzione all'Aritmetica Modulo N

Salvatore Capolupo - https://salvatorecapolupo.github.io/about-me/

April 16, 2025

Introduzione

L'aritmetica modulo N è un concetto fondamentale in matematica e informatica. Essa si basa sul calcolo del *resto* di una divisione intera. In altre parole, dato un numero a e un altro numero N, il risultato dell'operazione $a \mod N$ è il resto che otteniamo quando dividiamo a per N.

Formalmente, dato che $a \div N = q$ (quoziente) e r (resto), si ha:

$$a = N \cdot q + r, \quad \text{dove } 0 \leq r < N$$

In questo caso, il risultato dell'operazione modulo è proprio il resto r, che sarà ovviamente compreso nell'intervallo $[0, N)$ (il modulo di un numero per N avrà al massimo valore $N - 1$).

Questa operazione è utilizzata in numerosi contesti, come nella gestione dei numeri in base binaria, nella crittografia, nella gestione del tempo e altro ancora.

Cosa vuol dire "modulo"?

Quando calcoliamo il "modulo" di un numero, stiamo cercando il resto che otteniamo quando dividiamo quel numero per un altro numero.

Per esempio:

Se dividi 17 per 5, ottieni un quoziente di 3 e un resto di 2. Quindi, possiamo dire che 17 modulo 5 è uguale a 2.

Se dividi 23 per 7, ottieni un quoziente di 3 e un resto di 2. Quindi, possiamo dire che 23 modulo 7 è uguale a 2.

In generale, per calcolare il modulo di un numero, basta fare una divisione e vedere quanto "avanza" dopo aver fatto il quoziente. Tale "avanzo" sarà il risultato del modulo.

In sostanza se hai un numero a e vuoi calcolare $a \mod N$, fai la divisione di a per N e prendi il resto della divisione.

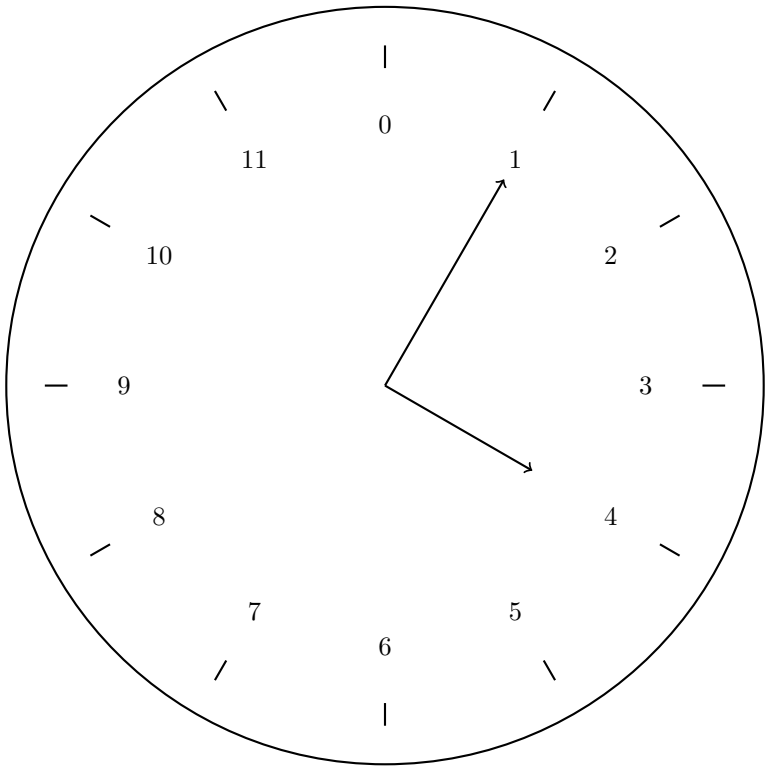
Esempi Pratici di Aritmetica Modulo N

Modulo 12: Le Lancette dell'Orologio

Un esempio comune di aritmetica modulo 12 è l'orologio. Le ore vanno da 1 a 12, e dopo le 12 si ricomincia da 1. In questo caso, possiamo pensare a un orologio che usa un sistema di numerazione modulo 12, dove dopo 12 ore, il conteggio riparte da 0, proprio come succede con i minuti (che vanno da 0 a 59).

- Se sono le ore 16, che ore sono?
  $16 \pmod{12} = 4$. Quindi saranno le 4.
- Se sono le 9 e passano 5 ore, che ore sono?
  $9 + 5 = 14$, ma $14 \pmod{12} = 2$. Quindi, saranno le 2.
- Se sono le 11 e passano 4 ore:
  $11 + 4 = 15$, e $15 \pmod{12} = 3$. Risultato: le 3.
- Se sono le 10 e passano 15 ore:
  $10 + 15 = 25$, ma $25 \pmod{12} = 1$. Risultato: l'ora è 1.

In questo caso, il modulo 12 aiuta a tenere traccia delle ore che ripartono ogni 12 ore, proprio come accade su un orologio. Qui il risultato modulo 12 è equivalente all'operazione di "riavvolgere" l'orologio quando superiamo le 12 ore.



In questo caso, i numeri sul quadrante rappresentano i minuti (da 0 a 59). Se aggiungiamo 5 minuti a 9 minuti, otteniamo 14, ma $14 \mod 12 = 2$, quindi il tempo diventa 2 minuti.

Modulo 2: Il Sistema Binario

Il modulo 2 è la base del sistema binario, che utilizziamo nei computer. Qui, i numeri sono rappresentati solo da 0 e 1. In aritmetica modulo 2:

$$0 + 1 = 1, \quad 1 + 1 = 0 \pmod 2 \text{ (con riporto di 1)} \tag{1}$$

La somma di due numeri binari avviene come in una somma "con riporto", proprio come quando sommiamo numeri in decimale:

```
function somma_binaria(a, b):
    risultato = (a + b) % 2
    riporto = (a + b) // 2
    return risultato, riporto
```

Modulo 16: Il Sistema Esadecimale

L'aritmetica modulo 16 viene utilizzata per rappresentare numeri nel sistema esadecimale, che usa i numeri da 0 a 15, dove i numeri 10-15 sono rappresentati

dalle lettere A-F. Esempi di congruenze in modulo 16:

- $10 \equiv A \pmod{16}$
- $11 \equiv B \pmod{16}$
- $15 \equiv F \pmod{16}$

Questo sistema è molto usato per rappresentare colori HTML, indirizzi di memoria e altro ancora.

Somma di giorni in modulo 28, 29, 30, 31

Quando lavoriamo con il calendario, dobbiamo spesso sommare giorni a una data specifica, tenendo conto dei diversi numeri di giorni in ciascun mese. L'aritmetica modulo è particolarmente utile per gestire questa somma, poiché i mesi del calendario hanno un numero variabile di giorni. Per esempio:

- Un mese di febbraio ha 28 giorni in un anno comune e 29 giorni in un anno bisestile, quindi possiamo utilizzare modulo 28 o modulo 29 a seconda del caso.
- I mesi di aprile, giugno, settembre e novembre hanno 30 giorni, quindi sono descritti da modulo 30.
- I mesi di gennaio, marzo, maggio, luglio, agosto, ottobre e dicembre hanno 31 giorni, quindi sono descritti da modulo 31.

Ad esempio, se oggi è il 28 febbraio in un anno comune (anno non bisestile), e vogliamo sapere che giorno sarà dopo 5 giorni, dobbiamo sommare 5 giorni e applicare modulo 28:

$$28 + 5 = 33, \quad 33 \pmod{28} = 5$$

Quindi, il 5 marzo sarà la data risultante. Spieghiamo ancora meglio: quando sommiamo 28 e 5 otteniamo 33. Tuttavia, se calcoliamo 33 mod 28, vogliamo trovare il resto che otteniamo dividendo 33 per 28. La divisione ci dà un quoziente di 1 e un resto di 5. Quindi, possiamo dire che:

$$28 + 5 = 33, \quad 33 \pmod{28} = 5$$

In altre parole, 33 mod 28 è uguale a 5, perché 33, diviso 28, lascia un resto di 5.

Un altro esempio: se oggi è il 30 aprile, e vogliamo sapere che giorno sarà dopo 10 giorni, dobbiamo sommare 10 giorni e applicare modulo 30:

$$30 + 10 = 40, \quad 40 \pmod{30} = 10$$

Quindi, il 10 maggio sarà la data risultante.

In generale, per sommare giorni a una data, bisogna tenere conto del modulo corrispondente al mese (30, 29, 28, o 31), applicare la somma e determinare la data finale tramite il resto della divisione per il modulo. Questa operazione ci consente di navigare facilmente nel calendario e di determinare date future senza doverci preoccupare di sbagliare data. Quando si programmano le app, ad esempio, è molto comune dover fare conti sul numero di giorni per garantire che uno script venga eseguito ogni X giorni, ad esempio, evitando errori nel passaggio da un mese al successivo.

Applicazioni Pratiche di Modulo N

L'aritmetica modulo N ha numerose applicazioni pratiche:

- **Modulo 3**: Viene usato in alcuni algoritmi di controllo e in operazioni di hashing.
- **Modulo 256**: Utilizzato nei calcoli di checksum e nei pacchetti di rete.
- **Modulo 1000**: Impiegato nelle operazioni finanziarie per arrotondamenti, come nei conti bancari.

Esercizi proposti

1. **Modulo 2 (Pari e Dispari)**: Calcola $14 \mod 2$. È un numero pari o dispari?
2. **Modulo 2 (Pari e Dispari)**: Calcola $37 \mod 2$. È un numero pari o dispari?
3. **Modulo 2 (Somma di Pari e Dispari)**: Se $a \equiv 0 \pmod 2$ e $b \equiv 1 \pmod 2$, calcola $a + b \mod 2$.
4. **Modulo 2 (Sottrazione di Pari e Dispari)**: Se $a \equiv 1 \pmod 2$ e $b \equiv 0 \pmod 2$, calcola $a - b \mod 2$.
5. **Modulo 2 (Moltiplicazione di Pari e Dispari)**: Se $a \equiv 0 \pmod 2$ e $b \equiv 1 \pmod 2$, calcola $a \times b \mod 2$.

1. **Modulo 6**: Calcola $45 \mod 6$.
2. **Modulo 5**: Calcola $14 \mod 5$.
3. **Modulo 7**: Calcola $50 \mod 7$.
4. **Modulo 9**: Calcola $57 \mod 9$.
5. **Modulo 8**: Calcola $64 \mod 8$.

6. **Modulo 10**: Se un numero è congruente a 7 modulo 10, quale sarà il valore di x se $x + 5 \equiv 0 \pmod{10}$?

7. **Modulo 12**: Se sono le 10:00, che ora sarà tra 17 ore? (Usa il modulo 12).

8. **Modulo 12**: Se sono le 3:00, che ora sarà tra 20 ore? (Usa il modulo 12).

9. **Modulo 16**: Calcola $28 \mod 16$.

10. **Modulo 20**: Se $a \equiv 7 \pmod{20}$ e $b \equiv 15 \pmod{20}$, calcola $a+b \mod 20$.

11. **Modulo 25**: Calcola $54 \mod 25$.

12. **Modulo 30**: Se oggi è il 15 febbraio, che giorno sarà tra 20 giorni? (Usa il modulo 30).

13. **Modulo 24**: Calcola $53 \mod 24$.

14. **Modulo 13**: Calcola $111 \mod 13$.

15. **Modulo 18**: Se $a \equiv 11 \pmod{18}$ e $b \equiv 8 \pmod{18}$, calcola $a-b \mod 18$.

16. **Modulo 15**: Calcola il risultato di $100 \mod 15$.

17. **Modulo 11**: Calcola $98 \mod 11$.

18. **Modulo 19**: Calcola $128 \mod 19$.

19. **Modulo 32**: Calcola $58 \mod 32$.

20. **Modulo 40**: Calcola il resto della divisione di 1234 per 40.

21. **Modulo 29**: Se $a = 25$ e $b = 10$, calcola $a + b \mod 29$.

22. **Modulo 7**: Se $a \equiv 2 \pmod{7}$ e $b \equiv 5 \pmod{7}$, calcola $a \times b \mod 7$.

23. **Modulo 50**: Calcola $86 \mod 50$.

24. **Modulo 60**: Se sono le 12:30 e voglio aggiungere 45 minuti, che ora sarà? (Usa il modulo 60).

25. **Modulo 25**: Se un numero è congruente a 18 modulo 25, calcola $18 + 10 \mod 25$.

26. **Modulo 20**: Se oggi è il 17 marzo e vuoi aggiungere 15 giorni, che giorno sarà? (Usa il modulo 20).

Esercizi con Applicazioni al Calendario

1. **Modulo 31**: Se oggi è il 25 luglio, che giorno sarà tra 50 giorni? (Usa modulo 31).
2. **Modulo 30**: Se oggi è il 5 aprile, che giorno sarà tra 60 giorni? (Usa modulo 30).
3. **Modulo 28**: Se oggi è il 12 febbraio, che giorno sarà tra 30 giorni? (Usa modulo 28).
4. **Modulo 29 (Anni Bisestili)**: Se oggi è il 28 febbraio di un anno bisestile, che giorno sarà tra 3 giorni? (Usa modulo 29).
5. **Modulo 31**: Se oggi è il 18 gennaio, che giorno sarà tra 40 giorni? (Usa modulo 31).

Esercizi con la Somma di Giorni

1. **Modulo 30**: Se oggi è il 25 novembre e voglio sapere che giorno sarà tra 45 giorni, quale data sarà? (Usa modulo 30).
2. **Modulo 29**: Se oggi è il 15 marzo, che giorno sarà tra 40 giorni? (Usa modulo 29).
3. **Modulo 28**: Se oggi è il 7 settembre, che giorno sarà tra 50 giorni? (Usa modulo 28).
4. **Modulo 31**: Se oggi è il 30 maggio, che giorno sarà tra 65 giorni? (Usa modulo 31).
5. **Modulo 30**: Se oggi è il 10 agosto, che giorno sarà tra 80 giorni? (Usa modulo 30).
6. **Modulo 12**: Se sono le 6:00, che ora sarà tra 25 ore? (Usa modulo 12).
7. **Modulo 31**: Se oggi è il 3 marzo, che giorno sarà tra 120 giorni? (Usa modulo 31).