

L'aritmetica dell'orologio

ovvero: congruenze modulo n

Lorenzo Mazza

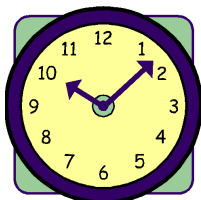
8 Febbraio 2024

Aritmetica dell'orologio

L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, \dots\}$.

L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.

una volta raggiunto l'ultimo numero si ricomincia dal primo.

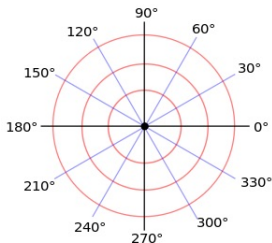


le 4 corrispondono anche alle 16 del pomeriggio

16 è congruo a 4 modulo 12

$$16 \equiv 4 \pmod{12}$$

La stessa cosa accade anche per i gradi di un angolo giro, in questo contesto è del tutto chiaro che 0 equivale a 360.



$$\begin{aligned}370 &\equiv 10 \pmod{360} \\750 &\equiv 30 \pmod{360} \\-90 &\equiv 270 \pmod{360}\end{aligned}$$

Possiamo estendere le congruenze ai numeri negativi, ad esempio:

$$-4 \equiv 8 \pmod{12}$$

A volte è utile ragionare così:

*Un bimbo nato in Novembre è stato concepito in ...
... aggiungo tre mesi ...
... Febbraio*

È più semplice aggiungere 3 mesi che sottrarne 9 e

$$+3 \equiv -9 \pmod{12}$$

Definizione di congruenza modulo n

Riassumendo quanto abbiamo visto, possiamo affermare che:

- 1 due numeri interi sono *congrui modulo n* se **hanno lo stesso resto nella divisione per n**

ESEMPIO: $13 \equiv 4 \pmod{3}$: infatti sia 13 sia 4 hanno resto 1 se divisi per tre.

ciò equivale a dire che:

- 2 due numeri interi sono *congrui modulo n* se **la loro differenza è un multiplo di n**

Nell'**ESEMPIO** precedente $13 - 4 = 9$ è un multiplo di 3.

DEFINIZIONE (congruenza modulo n)

Fissato un intero positivo n , siano a e b due numeri in \mathbb{Z} ,

$$a \equiv b \pmod{n} \iff \exists h \in \mathbb{Z} (a - b = hn)$$

TEOREMA

La congruenza modulo n è una relazione di equivalenza. Cioè soddisfa le seguenti proprietà:

- 1 Riflessiva: $a \equiv a \pmod{n}$
- 2 Simmetrica: Se $a \equiv b \pmod{n}$ allora $b \equiv a \pmod{n}$
- 3 Transitiva: Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ allora $a \equiv c \pmod{n}$

Operazioni e congruenze

Se il mio orologio segna le ore 8 del mattino e fra 35 ore ho un impegno importante a che ora sarò impegnato? Nessuno penserebbe di rispondere $8+35=43$ piuttosto

$$8+35=(8+24)+11=8+11=19$$

In generale la somma e la moltiplicazione “rispettano” la congruenza nel senso esplicitato dal seguente teorema.

TEOREMA Siano a, b, c, d numeri interi e n, k interi positivi fissati

$$a \equiv b \pmod{n}, c \equiv d \pmod{n} \implies \begin{cases} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \\ a^k \equiv b^k \pmod{n} \end{cases}$$

ESEMPIO Per calcolare $324 \cdot 231$ modulo 10, non è necessario svolgere effettivamente il prodotto, ma si possono sostituire i fattori con i termini equivalenti $4 \equiv 324 \pmod{10}$ e $1 \equiv 231 \pmod{10}$ ottenendo:

$$324 \cdot 231 \equiv 4 \cdot 1 \equiv 4 \pmod{10}$$

ESERCIZIO Determina, applicando il teorema precedente, **quale delle seguenti congruenze è corretta**:

- $7^2 + (5 \cdot 57) \equiv 40 \pmod{48}$;
- $2^4 + 5^{301} + (6 \cdot 31) \equiv 3 \pmod{5}$;
- $9^{2000} \equiv 1 \pmod{80}$;

NB Non è corretto passare ai moduli anche all'esponente!

Per esempio: $2^4 = 16$ *non* è congruo a 2^1 modulo 3

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, ... alla sua ultima cifra, la cifra delle unità.

ESERCIZIO

Determinare le **cifre delle unità** dei seguenti numeri:

$$2^{20}$$

$$23^{23}$$

$$2023^{2023}$$

La congruenza modulo 9: la somma delle cifre

Ogni numero intero positivo è congruo, modulo 9, alla somma delle sue cifre. Infatti un intero K di $n + 1$ cifre può essere scritto come:

$$K = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$$

e dato che $10 \equiv 10^2 \equiv \dots \equiv 10^n \equiv 1 \pmod{9}$, si ha

$$K \equiv a_0 + a_1 + a_2 + \dots + a_{n-1} + a_n := K'$$

Lo stesso ragionamento può essere ripetuto su K' e, dato che la congruenza è una relazione di equivalenza (**proprietà transitiva**), iterando si ottiene un numero di una sola cifra.

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n$$

possiamo ricavare i criteri di divisibilità:

per 3 e per 9 sia modulo 3 sia modulo 9 si ha:

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n \equiv a_0 + a_1 + \dots + a_n$$

per 2 e per 5 Dato che, per $n \geq 1$, si ha $10^n \equiv 0$ abbiamo, sia modulo 2 sia modulo 5:

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n \equiv a_0$$

per 11 Dato che, se $n \in \mathbb{N}$, $10^{2n+1} \equiv -1 \pmod{11}$ e $10^{2n} \equiv 1 \pmod{11}$, otteniamo

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n \equiv a_0 - a_1 + a_2 - \dots + (-1)^n a_n$$

Congruenze e quadrati perfetti

È possibile caratterizzare i quadrati perfetti con le congruenze. Ricordando infatti che un qualunque quadrato perfetto è della forma $4k$ (se la base è pari) o $4k + 1$ (se la base è dispari), risulta allora che:

- il quadrato di un intero pari è sempre congruo a 0 modulo 4;
- il quadrato di un intero dispari è sempre congruo a 1 modulo 4;

Congruenze e quadrati perfetti

ESERCIZIO

Un numero si dice moderno se, in base 10, può essere espresso concatenando un po' di scritture decimali di 2006: ad esempio, 200620062006 è moderno, mentre 20200606 e 2006200 non lo sono. Quante cifre ha il più piccolo quadrato perfetto moderno positivo? (Gara provinciale di Febbraio 2006)

ALTRI ESERCIZI

- 1 Qual è il resto della divisione per 37 del numero 6^{1987} ?
- 2 Determinare le ultime due cifre del numero 307^{46}
- 3 Due persone sono nate in anni diversi ma festeggiano il compleanno lo stesso giorno. Se la somma delle loro età attuali è dispari, negli anni futuri la somma delle loro età sarà pari o dispari? E il prodotto? Se il prodotto delle loro età attuali è dispari, negli anni futuri la somma delle loro età sarà pari o dispari?
- 4 Dimostrare che $7|(3^{2n+1} + 2^{n+2})$ per ogni numero naturale n .
- 5 Dimostra che $7|(2222^{5555} + 5555^{2222})$.
- 6 Dimostra che, comunque si scelgano a, b, c interi, risulta che se $21|100a + 10b + c$ allora $21|a - 2b + 4c$.
- 7 Provare che, per ogni n naturale, risulta $11^{n+2} + 12^{2n+1}$ divisibile per 133.