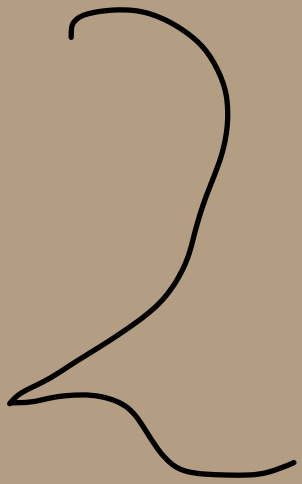
Aritmetica Modulare



ARITMETICA MODULARE: • RIGUARDA IL CALCOLO SUI RESTI DELLE DIVISIONI TRA INTERI RISPETTO AD UN DIVISORE FISSATO

NUMERI EQUIVALENTI: • Numeri interi con lo stesso resto rispetto ad un divisore fisso vengono considerati equivalenti

$$a \equiv b \pmod m \iff (a \bmod m) = (b \bmod m)$$

(a è congruo a b modulo m)

$a \not\equiv b \pmod m$ "non congruo"

$a \equiv a \pmod m \quad \forall m$ RELAZIONE RIFLESSIVA

Ex.
- $12 \equiv 9 \pmod 3$ $\quad 12 \% 3 = 0 \wedge 9 \% 3 = 0$
- $-15 \equiv 9 \pmod 4$ $\quad -15 \% 4 = 1 \wedge 9 \% 4 = 1$
- $7 \not\equiv 1 \pmod 4$ $\quad 7 \% 4 = 3 \wedge 1 \% 4 = 1$
- $1 \equiv 1 \pmod 3$ $\quad 1 \% 3 = 1 \wedge 1 \% 3 = 1$

$a \equiv a \bmod m \pmod m$

Ex. $10 \equiv 10 \bmod 3 \pmod 3$

$10 \equiv 1 \pmod 3$ $\quad 10 \% 3 = 1 \wedge 1 \% 3 = 1$

RELAZIONE DI CONGRUENZA: • $a \equiv b \pmod m \implies a - b$ è un multiplo di m

LA CONGRUENZA È UNA RELAZIONE DI EQUIVALENZA

- vale la proprietà riflessiva $\forall a \in \mathbb{Z} : a \equiv a \pmod m$
- " " " simmetrica $\forall a, b \in \mathbb{Z} : a \equiv b \pmod m \to b \equiv a \pmod m$
- " " " transitiva $\forall a, b, c \in \mathbb{Z}\ a \equiv b \pmod m \wedge b \equiv c \pmod m \implies a \equiv c \pmod m$

└ Ci sono m classi di equivalenza $[0] \dots [m-1]$

CONGRUENZA MODULO 0 $a \equiv b \pmod 0 \iff a - b = 0 \implies a = b$

in questo caso ogni classe contiene un solo elemento $\in \mathbb{Z}$ (singoletto)

e ci sono ∞ classi $[0] \dots [\infty]$

CONGRUENZA MOD 1: $a \equiv b \pmod 1 \iff a - b = 1$ ovvero $a - b$ è un multiplo di 1.
ma ogni numero è multiplo di 1 $\Rightarrow \forall a \in \mathbb{Z}$ è multiplo con ogni numero $\Rightarrow$ ∃ una sola classe di equivalenza contenente tutti gli interi ovvero $\mathbb{Z}$

CONGRUENZA MOD 2: $a \equiv b \pmod 2 \iff a - b = 2$ ovvero $a - b$ è un numero pari.
il resto r $0 \leq r < 2$ $(0, 1)$ $\Rightarrow$ abbiamo solo due classi, una con i numeri pari e una con i numeri dispari

$$[a]_m = \{ b \in \mathbb{Z} : a \equiv b \pmod m \}$$

I RESTI DI UNA DIVISIONE MOD m $[0, m-1]$

STABILIRE LA CLASSE DI EQUIVALENZA DI $a \in \mathbb{Z}$: $[a]_m = [r]_m$ dove $r = a \,\%\, m$

Ex. Se $m = 5$ e $a = 22$ $\quad a \,\%\, m = 22 \,\%\, 5 = 2$
$\Rightarrow [22]_5 = [2]_5$

NELLA CLASSE $[0]_m$ CI SONO TUTTI I MULTIPLI DI m

TEOREMA: Dato $a \equiv b \pmod m$ ∧ $c \equiv d \pmod m$ abbiamo:
1. $a + c \equiv b + d \pmod m$
2. $a \cdot c \equiv b \cdot d \pmod m$

INVARIANZA RISPETTO

- **LA SOMMA** → vale anche per la differenza
  se $a \equiv b \pmod m$ allora $a + c \equiv b + c \pmod m$ $\quad \forall a, b, c \in \mathbb{Z}$
- **IL PRODOTTO** se $a \equiv b \pmod m$ allora $a \cdot c \equiv b \cdot c \pmod m$ $\quad \forall a, b, c \in \mathbb{Z}$
  → per la divisione non vale sempre

PROPRIETÀ

(P1) Dati $a, b, m \in \mathbb{N}$ visto che $a \equiv a \bmod m \pmod m$ e $b \equiv b \bmod m \pmod m$
$\Rightarrow (a + b) \equiv (a \bmod m + b \bmod m) \pmod m$

(P2) Dati $a, n, m \in \mathbb{N}$ visto che $a \equiv a \bmod m \pmod m$
$\Rightarrow a^n \equiv (a \bmod m)^n \pmod m$

(P3) Dati $a, b, h, k \in \mathbb{N}$
$\Rightarrow a^h \cdot b^k \equiv (a^h \bmod m)(b^k \bmod m) \pmod m$ quindi: $a^h \cdot b^k \bmod m = (a \bmod m)^h \cdot (b \bmod m)^k \bmod m$

ESEMPI SLIDE 99

TEOREMA: Una sequenza di m numeri consecutivi contiene un numero divisibile per m

DIM SLIDE 101

- Dati 2 numeri consecutivi, almeno uno di due è divisibile per 2
- // 3 // //, // // // // // // // 3 e almeno uno per 2 $\Rightarrow$ il prodotto di 3 numeri consecutivi è divisibile per 6
- // 5 // //, // // // // // // // per 5, almeno uno per 3 e almeno 2 per 2 $\Rightarrow$ il prodotto di 5 numeri consecutivi è divisibile per 60
- Così via

$\forall n > 1 \Rightarrow n^3 - n \equiv 0 \pmod 6$ ovvero $n^3 - n$ è un multiplo di 6

ESERCIZI SLIDE 104

INVERSO DI UN NUMERO NELL'ARITMETICA MODULARE: Siano $a, b \in \mathbb{N}$ $a, b > 0 \Rightarrow \exists\, x \in \mathbb{N} \mid a \cdot x \equiv 1 \pmod b$ $\Leftrightarrow$ a e b sono coprimi

- l'elemento x è denotato con a^{-1}
- a^{-1} viene detto "inverso di a modulo b"

Esempi

$a = 5, b = 3 \Rightarrow a^{-1} = 2$ perché $2 \cdot 5 \bmod 3 = 10 \bmod 3 = 1$

$a = 9, b = 11 \Rightarrow a^{-1} = 5$ perché $5 \cdot 9 \bmod 11 = 45 \bmod 11 = 1$

$a = 9, b = 7 \Rightarrow a^{-1} = 4$ perché $4 \cdot 9 \bmod 7 = 36 \bmod 7 = 1$

$a = 14, b = 6$ (non sono coprimi) $\nexists\, a^{-1}$

FUNZIONE DI EULERO ϕ: Serve a calcolare quanti numeri coprimi sono compresi fra 1 e n.

$$\phi(n) = \left\{ x \in \mathbb{N} \mid 0 < x \leq n, MCD(n, x) = 1 \right\}$$

ϕ DI UN NUMERO PRIMO: $\phi(n) = n - 1$

ϕ DI UN QUALSIASI NUMERO: un numero può essere scritto come prodotto di numeri primi.

$n = p_1 \cdot \ldots \cdot p_r \qquad \phi(n) = \phi(p_1) \cdot \ldots \cdot \phi(p_r)$

$\phi(n^k)$: $\phi(n^k) = n^k - n^{k-1}$

FORMULA GENERALE: $\phi(n) = (p_1^{k_1} - p_1^{k-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_m^{k_m} - p_m^{k_m-1})$ DIM SLIDE 115

PICCOLO TEOREMA DI FERMAT: Se p è primo ed è coprimo con a allora $a^{p-1} \equiv 1 \pmod p$

Ex. $p=3, a=10$: $10^2 \bmod 3 \equiv 1 \bmod 3$
↳ $100 \bmod 3 = 1$

$p=5, a=12$: $12^4 \bmod 5 \equiv 1 \bmod 5$

CONSEGUENZA TEOREMA D'EULERO: Se a, n sono coprimi, per $\forall x > 0$:
$a^x \equiv a^{x \bmod \phi(n)} \pmod n$ DIM SLIDE 127

Ex. $12^{50} \bmod 5 \equiv 12^{50\% \phi(5)} \bmod 5 \equiv 12^{50\%4} \bmod 5 \equiv 12^2 \bmod 5 \equiv 144 \bmod 5 = 4$
ALTRI ESEMPI SLIDE 128

CALCOLO INVERSO MODULARE: Se n e m sono coprimi l'inverso modulare si calcola:

$(n \bmod m)^{\phi(m)-1} \bmod m$

Ex trovare $\bar{a}^1$ di $11\%7$.

$(11 \bmod 7)^5 \bmod 7 \equiv 4^5 \bmod 7 \equiv (4^2)^2 \bmod 7 \cdot 4 \bmod 7 \equiv (16 \bmod 7)^2 \cdot 4 \bmod 7 \equiv$
$\equiv 2^2 \cdot 4 \bmod 7 \equiv 4 \cdot 4 \bmod 7 \equiv 16 \bmod 7 = 2$

VERIFICA
$11 \cdot 2 \equiv 1 \bmod 7$ perché $22 \bmod 7 = 1 \wedge 1 \bmod 7 = 1$

PROVA DEL 9: Serve a dire se un calcolo è sbagliato, ma non ci assicura che sia giusto

Ex. $123 \cdot 347 = 42691$ Giusto? $P(123)=6$ $P(347)=5$ $\Longrightarrow$ $P(6 \cdot 5)=3$
$P(42691)=2$ ↳ Il calcolo è sbagliato

DIM SLIDE 137

CODICE ISBN Slide 139 e 140

CODICE CARTA DI CREDITO: Slide 141

CIFRARIO DI CESARE: Slide 143

ROOT-13: Slide 144

SEQUENZE NUMERICHE: DA SLIDE 148