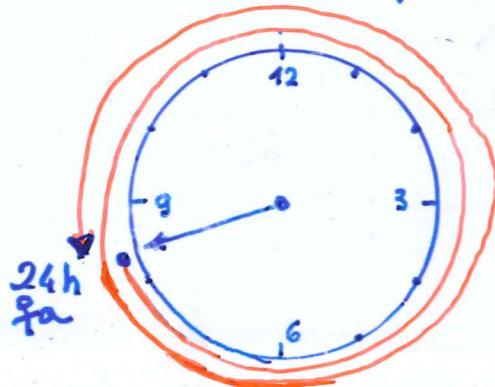


Congruenze in \mathbb{Z} : l'aritmetica dell'orologio

(85)

Sono le 8:30. Che ore saranno tra 59 ore e $\frac{3}{4}$? Che ore erano 101 ore fa? Sono problemi che hanno a che fare con le congruenze in \mathbb{Z} : ogni 24 ore sull'orologio si legge la stessa ora e quindi è indifferente chiedersi che ore erano 101 ore fa o $101 - 24 \cdot 4 = 5$ ore fa.

Generalizzando da 24 a $n \in \mathbb{Z}$, $n > 1$ si arriva alla



DEF. Siano $a, b \in \mathbb{Z}$ e $n \in \mathbb{Z}$, $n > 1$.

Si dice che a è congruo a b modulo n

$$a \equiv b \pmod{n}$$

se $a - b$ è divisibile per n , cioè $\exists k \in \mathbb{Z}$ t.c.
 $a - b = kn$.

PROP. La congruenza è una rel. di eq. in \mathbb{Z} .

Dimo. 1. $a \equiv a \pmod{n}$ poiché $a - a = 0 \cdot n$

2. $a \equiv b \pmod{n} \Rightarrow \exists k \in \mathbb{Z}$ t.c. $a - b = kn \Rightarrow b - a = (-k)n \Rightarrow b \equiv a \pmod{n}$

3. $a \equiv b \pmod{n} \Rightarrow \exists k \in \mathbb{Z}$ t.c. $a - b = kn$
 $b \equiv c \pmod{n} \Rightarrow \exists h \in \mathbb{Z}$ t.c. $b - c = hn$

e sommando membro a membro:

$$(a - b) + (b - c) = kn + hn \Leftrightarrow a - c = (k+h)n \Rightarrow a \equiv c \pmod{n}$$

■

La classe di congruenza di a è:

$$[a]_n = \{x \in \mathbb{Z} \text{ t.c. } x = a + kn, k \in \mathbb{Z}\}$$

Prendiamo ad esempio $n=4$ e le classi di congruenza mod 4

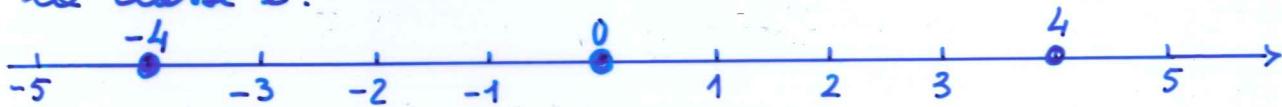
$$a \equiv b \pmod{4} \Leftrightarrow a - b = 4k, k \in \mathbb{Z}$$

$$\Leftrightarrow a = b + 4k$$

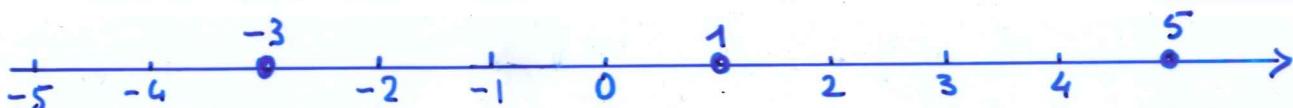
Considero

$$[0]_4 = \{ \dots, -8, -4, 0, 4, 8, \dots \} \quad \begin{array}{l} \text{numerazione} \\ \text{per 4 a partire} \\ \text{da 0} \end{array}$$

la classe è:



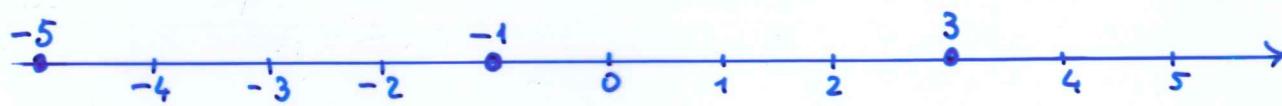
$$[1]_4 = \{ \dots, -11, -7, -3, 1, 5, 9, 13, \dots \} \quad \begin{array}{l} \text{numeraz. per 4} \\ \text{a partire da 1} \end{array}$$



$$[2]_4 = \{ \dots, -10, -6, -2, 2, 6, 10, \dots \} \quad \begin{array}{l} \text{numeraz. per 4} \\ \text{a partire da 2} \end{array}$$



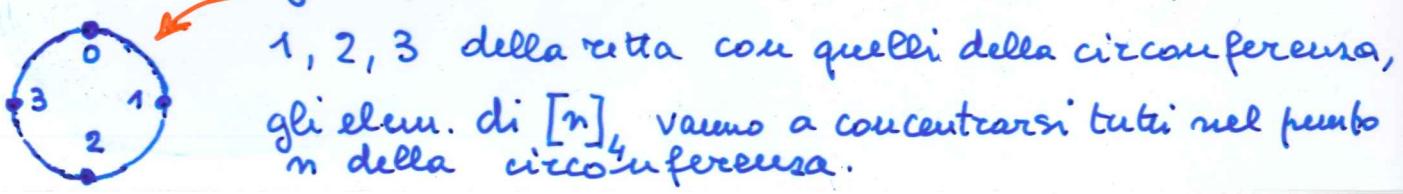
$$[3]_4 = \{ \dots, -9, -5, -1, 3, 7, 11, \dots \} \quad \begin{array}{l} \text{numeraz. per 4} \\ \text{a partire da 3} \end{array}$$



Tutti i punti della retta "intera" stanno in una delle 4 classi di congruenza e in una sola.

Gli elementi di $\frac{\mathbb{Z}}{4}$ sono i 4 insiemini di punti.

Se avvolgo ciascuna delle rette su cui ho rappresentato gli elementi delle 4 classi di congruenza su una circonferenza lunga 4, in modo da far coincidere i punti 0, 1, 2, 3 della retta con quelli della circonferenza,



Quante sono le classi di congruenza modulon (85)
tre loro distinte?

Iniziamo con un esempio: sia $n=3$

$$0 \equiv_3 3 \equiv_3 6 \equiv_3 -3 \equiv \dots \Rightarrow [0]_3 = \{0 + 3k, k \in \mathbb{Z}\}$$

$$1 \equiv_3 4 \equiv_3 7 \equiv_3 -2 \equiv \dots \Rightarrow [1]_3 = \{1 + 3k, k \in \mathbb{Z}\}$$

$$2 \equiv_3 5 \equiv_3 8 \equiv_3 -1 \equiv \dots \Rightarrow [2]_3 = \{2 + 3k, k \in \mathbb{Z}\}$$

... è abbastanza ragionevole che non ce ne siano altre.

In effetti:

Prop. Fissato $n > 1$ ci sono esattamente n classi di congruenza modulo n , corrispondenti ai possibili resti nella divisione per n . Il loro insieme viene denotato con \mathbb{Z}_n e chiamato insieme delle classi di resti modulo n .

Dim. L'algoritmo della divisione garantisce che

$$\forall x \in \mathbb{Z} \quad \exists \text{ s.t. } q, r \text{ t.c. } x = nq + r, 0 \leq r < n.$$

Quindi ogni $x \in \mathbb{Z}$ appartiene a una delle n classi $[x]_n$.

Tali classi sono distinte poiché se $0 \leq r < s < n$

$$[r]_n = [s]_n \Rightarrow 0 \leq s - r < n \quad \text{e } s - r \text{ divisibile per } n$$

\Downarrow
il resto nella
divisione per
 n è $s - r$ \Downarrow
il resto nella
divisione per
 n è 0

$$\Rightarrow s = r.$$

Il rappresentante "naturale" di una classe di resti è il "resto", anche se va bene anche un elemento ad esso congruente mod n . Ad es

$$[1]_3 = [4]_3 = [-2]_3$$

ma di solito preferisco il primo.

$\forall x \in \mathbb{Z}$ $\exists q, r$ t.c. $x = qn + r$ $0 \leq r < n$

$$\Rightarrow x - r = qn \Rightarrow n | x - r$$

$$\Rightarrow [x]_n = [r]_n$$

i resti sono $\frac{0, 1, \dots, n-1}{n} \Rightarrow n$ classi
sono tutte distinte?

non lo siano. Ho trovato due resti

$$0 \leq r \leq s < n$$

t.c.

$$[r]_n = [s]_n$$

Considero $0 \leq s - r < n$

Dunque $s - r \mid n$

$$s - r = 0 \cdot n + \frac{s - r}{\text{resto}}$$

Ma $[r]_n = [s]_n \Leftrightarrow r \equiv s \pmod{n} \Leftrightarrow$
 $s - r = nq \Leftrightarrow n | s - r$
 $\Leftrightarrow \underline{\text{resto}} \text{ nelle divisione di } s - r$
 $\text{per } n \text{ è } \underline{\text{zero}}$

$$\Rightarrow s - r = 0 \Rightarrow s = r$$

Rivisitazione della dim. delle PROP. svolta a lezione

Prop. La relazione di congruenza mod n in \mathbb{Z}_n è
compatibile con le operazioni di somma e prodotto
definite in \mathbb{Z} , cioè se $a, b, c, d \in \mathbb{Z}$ e

$$a \equiv b \text{ mod } n, c \equiv d \text{ mod } n \Rightarrow a+c \equiv b+d \text{ mod } n$$

$$\exists k \in \mathbb{Z} \mid a-b = kn \quad \exists h \in \mathbb{Z} \mid c-d = hn \quad ac \equiv bd \text{ mod } n$$

Dimm. $(a+c) - (b+d) = (a-b) + (c-d) = kn + hn = (k+h)n$
 $\Rightarrow a+c \equiv b+d \text{ mod } n$

$$\left. \begin{array}{l} a = b + kn \\ c = d + hn \end{array} \right\} \Rightarrow ac = bd + (bh + dk + hn) n \Rightarrow ac \equiv bd \text{ mod } n$$

■

Ciò permette di definire una somma e un
prodotto in \mathbb{Z}_n :

$$[a]_n + [b]_n \stackrel{\text{DEF}}{=} [a+b]_n$$

$$[a]_n \cdot [b]_n \stackrel{\text{DEF}}{=} [ab]_n$$

Trovare la tavola delle due operazioni in \mathbb{Z}_4 e in \mathbb{Z}_5

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	0	1	2	3
$[1]_4$	1	2	3	0
$[2]_4$	2	3	0	1
$[3]_4$	3	0	1	2

\cdot	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	0	0	0	0
$[1]_4$	0	1	2	3
$[2]_4$	0	2	0	2
$[3]_4$	0	3	2	1

$[1]_4$ neutro
risp.

per comodità trascriviamo $[]_4$ nel riportare i risultati
Che cosa si nota? $[2]_4, [2]_4 = [0]_4$

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	0	1	2	3	4
$[1]_5$	1	2	3	4	0
$[2]_5$	2	3	4	0	1
$[3]_5$	3	4	0	1	2
$[4]_5$	4	0	1	2	3

\cdot	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	0	0	0	0	0
$[1]_5$	0	1	2	3	4
$[2]_5$	0	2	4	1	3
$[3]_5$	0	3	1	4	2
$[4]_5$	0	4	3	2	1

Che cosa si nota?

$[1]_5$ funziona da elemento
neutro risp.
e ogni classe $\neq [0]_5$ ha reciproco.

Come si calcola \equiv_4 ($0 \equiv_5$)?

Giuanzi tutto conviene cercare il resto (mod 4) (*)

Ad es.

$$2 \cdot 5 \equiv_4 ? \quad 5 = 1 \cdot 4 + 1 \Rightarrow 5 \equiv_4 1$$

$$2 \cdot 5 \equiv_4 2 \cdot 1 = 2$$

$$35 \cdot 17 \equiv_4 ? \quad 35 = 8 \cdot 4 + 3 \Rightarrow 35 \equiv_4 3$$

$$17 = 4 \cdot 4 + 1 \Rightarrow 17 \equiv_4 1$$

$$35 \cdot 17 \equiv_4 3 \cdot 1 = 3$$

Passando alle operazioni sulle classi di resto:

$$[2]_4 \cdot [2]_4 = [2 \cdot 2]_4 = [4]_4 = [0]_4$$

$$[2]_5 \cdot [3]_5 = [2 \cdot 3]_5 = [6]_5 = [1]_5$$

$$[3]_5 + [4]_5 = [3+4]_5 = [7]_5 = [2]_5$$

$$[4]_5 + [1]_5 = [4+1]_5 = [5]_5 = [0]_5$$

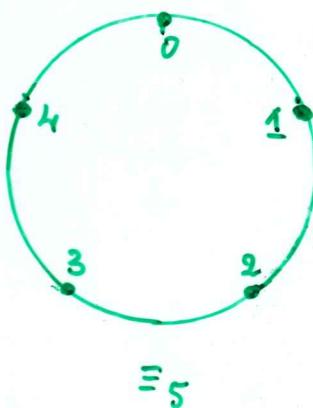
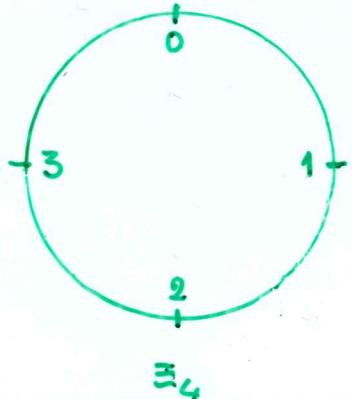


$$[4]_5 = -[1]_5$$

$$[3]_5 = ([2]_5)^{-1}$$

ecc.

(*) Per capire fisicamente che cosa si fa usare l'aritmetica dell'orologio con sole 4 (o 5) ore. Si noti l'analogia



con quel che si fa nel calcolo delle radici 4^e (o 5^e) di un numero complesso

HIP: $a, b, c \in \mathbb{Z}_n$, $n \in \mathbb{Z}$, $n > 1$

87ter

TH: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$

l'infatti

$$\begin{aligned} [a+b]_n + [c]_n &= [(a+b)+c]_n = \text{*ass in } \mathbb{Z}*} \\ &= [a+(b+c)]_n = [a]_n + [b+c]_n = \\ &= [a]_n + ([b]_n + [c]_n) \end{aligned}$$

cioè in \mathbb{Z}_n vale la pr. associativa della somma.

Allo stesso modo posso provare che valgono le propz.

- associativa del prodotto
- commutativa della somma e del prodotto
- distributiva del prodotto rispetto alla somma.

$[0]_n$ è neutro rig. + in \mathbb{Z}_n poiché:

$$\forall a \in \mathbb{Z} \quad [a]_n + [0]_n = [a+0]_n = [a]_n$$

$[1]_n$ è neutro rig. \circ in \mathbb{Z}_n poiché:

$$\forall a \in \mathbb{Z}: [a]_n \cdot [1]_n = [a \cdot 1]_n = [a]_n$$

$\exists x \in \mathbb{Z}_n$ t.c. $[a]_n + [x]_n = [0]_n$? cioè $\forall [a]_n \in \mathbb{Z}_n$ esiste l'opposto?

$$[a+x]_n = [0]_n$$

se ho scelto a con $0 \leq a < n$ conviene osservare
che $[0]_n = [u]_n \Rightarrow a+x = u \Leftrightarrow$ perf'ca
 $x = n-a$

$$[x]_n = [n-a]_n$$

con $n-a$ che è ancora un res

Oss. $n > 1$, $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Se $a \equiv b \pmod{n}$

allora

$$1. a^m \equiv b^m \pmod{n}$$

$$2. n|a \Leftrightarrow n|b$$

Dimo. 1. per la prop. a pag 87: $a^2 \equiv b^2 \pmod{n}$.

Giultra per le stessa prop.: se $a^{m-1} \equiv b^{m-1} \pmod{n}$
 $a \cdot a^{m-1} \equiv b \cdot b^{m-1} \pmod{n}$.

Per induzione si ha la tesi

$$2. a \equiv b \pmod{n} \Leftrightarrow b = a + kn \text{ con } k \in \mathbb{Z}$$

$$\begin{array}{l} \swarrow \\ n|a \Leftrightarrow a = hn \text{ con } h \in \mathbb{Z} \end{array}$$

$$b = hn + kn = (h+k)n \Rightarrow n|b$$

e simmetricamente per $n|b \Rightarrow n|a$. ■

Ne conseguono alcuni ben noti criteri di divisibilità:

Sia $a = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$, $a_k \neq 0$

- $2|10$, cioè $10 \equiv 0 \pmod{2}$, implica $10^m \equiv 0 \pmod{2}$

Quindi

$$a \equiv a_0 + \underbrace{0 + \dots + 0}_{\text{taddendi}} \pmod{2} \Rightarrow \boxed{2|a \Leftrightarrow 2|a_0}$$

$a_0 = 0, 2, 4, 6, 8$

- $5|10$, cioè $10 \equiv 0 \pmod{5}$, implica $10^m \equiv 0 \pmod{5}$

Quindi

$$a \equiv a_0 + 0 + \dots + 0 \pmod{5} \Rightarrow \boxed{5|a \Leftrightarrow 5|a_0}$$

$a_0 = 0, 5$

- $10 \equiv 0 \pmod{10} \Rightarrow 10^m \equiv 0 \pmod{10}$

$$\text{Quindi } a \equiv a_0 + 0 + \dots + 0 \pmod{10} \Rightarrow \boxed{10|a \Leftrightarrow 10|a_0}$$

$a_0 = 0$

$$- 100 \equiv 0 \pmod{100} \Rightarrow 10^m = 10^{m-2} \cdot 100 \equiv 0 \pmod{100} \quad (89)$$

$\forall m \geq 2$

Quindi $a \equiv a_0 + a_1 \cdot 10 + \underbrace{0 + \dots + 0}_{k-1 \text{ addendi}} \pmod{100} \Rightarrow$

$$\Rightarrow 100 | a \Leftrightarrow 100 | a_0 + a_1 \cdot 10 \Leftrightarrow a_0 = a_1 = 0$$

$$- 10 \equiv 1 \pmod{3} \Rightarrow 10^m \equiv 1^m = 1 \pmod{3}$$

Quindi

$$a \equiv a_0 + a_1 + \dots + a_R \pmod{3} \text{ e}$$

$$\boxed{3 | a \Leftrightarrow 3 | (a_0 + a_1 + \dots + a_R)}$$

$$- 10 \equiv 1 \pmod{9} \Rightarrow 10^m \equiv 1 \pmod{9}$$

Quindi

$$a \equiv a_0 + a_1 + \dots + a_R \pmod{9} \text{ e}$$

$$\boxed{9 | a \Leftrightarrow 9 | (a_0 + a_1 + \dots + a_R)}$$

$$- 10 \equiv -1 \pmod{11} \Rightarrow 10^{2k} \equiv 1 \pmod{11}$$

$$10^{2k+1} \equiv -1 \pmod{11}$$

Quindi

$$a \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^R a_R \pmod{11} \text{ e}$$

$$\boxed{11 | a \Leftrightarrow 11 | (a_0 - a_1 + a_2 - \dots + (-1)^R a_R)}$$

- Divisibilità per 7?

$$10 \equiv \frac{3}{7}, \quad 10^2 \equiv \frac{3 \cdot 10}{7} \equiv \frac{2}{7}, \quad 10^3 \equiv \frac{2 \cdot 10}{7} \equiv \frac{-1}{7}$$

$$10^4 \equiv \frac{-10}{7} \equiv \frac{-3}{7}, \quad 10^5 \equiv \frac{-30}{7} \equiv \frac{-2}{7}, \quad 10^6 \equiv \frac{-20}{7} \equiv \frac{1}{7}$$

$$\Rightarrow a \equiv \frac{a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6}{7} \pmod{7}$$

$$\Rightarrow 7 | a \Leftrightarrow 7 | \dots$$

Esercizi.

1. Stabilize quale è il resto nella divisione per 11 di $a=37.524.869$

- $a \equiv_{11} 9-6+8-4+2-5+7-3 = 8$

significa $a = 11k + 8 \Rightarrow$ Resto = 8.

2. Stabilire se è possibile che risulti

$$13.623 \times 8.431 = 114.845.513$$

- ordine di grandezza OK
- cifra delle unità OK
- PROVA DEL NOVE:

$$13.623 \times 8.431 \equiv_9 6 \times 7 \equiv_9 6 \text{ diversi}$$

$$114.845.513 \equiv_9 6+8+9+9 \equiv_9 5$$

Risposta: NO

E che sia $= 114.846.513$? Risposta: è possibile

.... Però è falso. $114.855.513$ è il prodotto VERO.

Cioè se $a \cdot b = c$ allora $[a]_9 \cdot [b]_9 = [c]_9$

ma se $[a]_9 \cdot [b]_9 = [c]_9$ non è detto che sia $a \cdot b = c$.

Lo stesso discorso si può fare nelle somme, le differenze e i quozienti

Come potrei verificare che 114.846.513 non è prodotto di 13.623×8.431 ?

Potrei verificare se funziona la prova "dell'11"

$$a = 13.623 \times 8.431 \equiv_{11} (3-2+6-3+1) \times (1-3+4-8) = 5 \times (-6) \equiv_{11} 3$$

invece

$$b = 114.846.513 \equiv_{11} 3-1+5-6+4-8+4-1+1 \equiv_{11} 1$$

Cioè il resto nella divisione per 11 dei due numeri a e b è diverso e quindi $a \neq b$

Invece

$$c = 114.855.513 \equiv_{11} 8-1+5-5+5-8+4-1+3 = 3$$

Il che non significa che abbiamo "provato" che 114.855.513 è il prodotto... solo che potrebbe esserlo

Generalizzazione dell'osservazione fatta nell'esercizio 1

Il metodo usato per stabilire criteri di divisibilità serve per trovare il resto nella divisione per 3, 9, 11, 7... (nel caso delle divisibilità il resto è zero).

Supponiamo se

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 \quad (\text{ad es. se } m=2)$$

$$\text{e } 10 = nq_1 + r_1 \text{ con } 0 \leq r_1 < n, \quad 10^2 = nq_2 + r_2 \text{ si ha}$$

$$a = a_0 + nq_1 \cdot a_1 + a_1 r_1 + nq_2 a_2 + a_2 r_2 =$$

$$= a_0 + a_1 r_1 + a_2 r_2 + n(q_1 a_1 + q_2 a_2)$$

Se $a_0 + a_1 r_1 + a_2 r_2$ non è $< n$, il resto r che si ottiene dividendo questa somma per n coincide con il resto nella divisione di a per n poiché

$$\text{se } a_0 + a_1 r_1 + a_2 r_2 = nq + r \quad 0 \leq r < n$$

$$\text{si ha } a = n(q + q_1 a_1 + q_2 a_2) + r.$$