Il codice ISBN e le cifre di controllo

applicazioni dell'aritmetica modulare

Claudio Bernardi Antonio Veredice

24 Marzo 2017

Aritmetica dell'orologio

L'aritmetica "ordinaria" ...

Aritmetica dell'orologio

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

Aritmetica dell'orologio

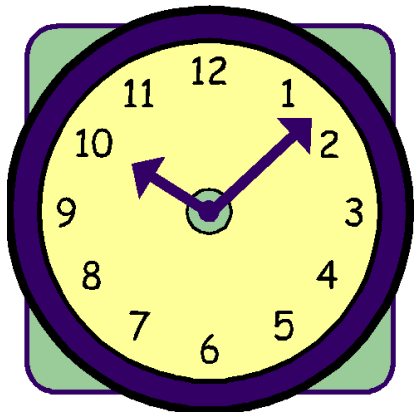
L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L' "aritmetica dell'orologio" ...

Aritmetica dell'orologio

L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.

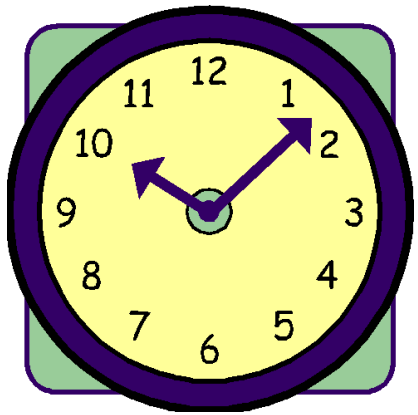
Aritmetica dell'orologio

L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.
una volta raggiunto l'ultimo numero si ricomincia dal primo.



Aritmetica dell'orologio

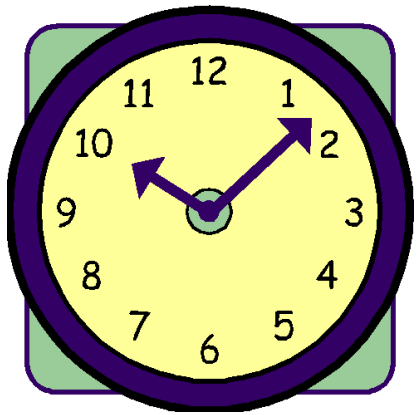
L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.
una volta raggiunto l'ultimo numero si ricomincia dal primo.



le 4 corrispondono anche alle 16 del pomeriggio

Aritmetica dell'orologio

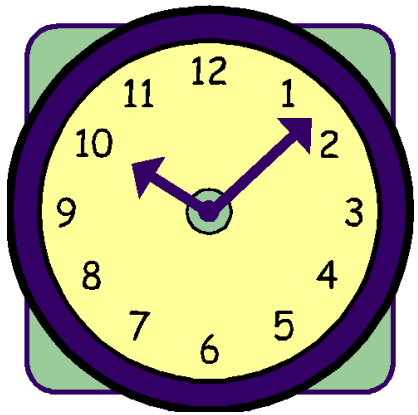
L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.
una volta raggiunto l'ultimo numero si ricomincia dal primo.



le 4 corrispondono anche alle 16 del pomeriggio
16 è congruo a 4 modulo 12

Aritmetica dell'orologio

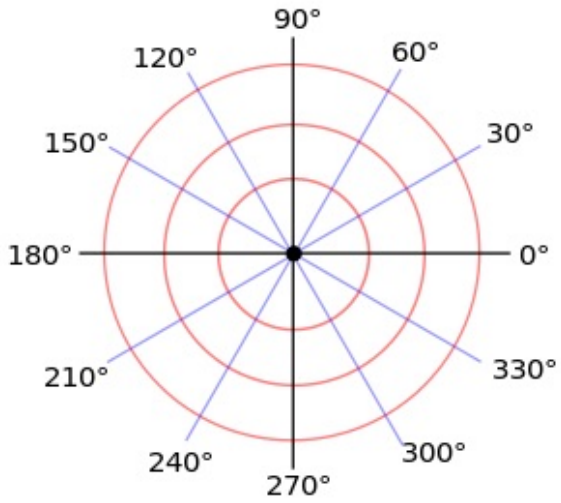
L'aritmetica "ordinaria" ... opera su insiemi infiniti $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$ o $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, ...\}$.
L'"aritmetica dell'orologio" ... ha solo 12 o 24 ore.
una volta raggiunto l'ultimo numero si ricomincia dal primo.



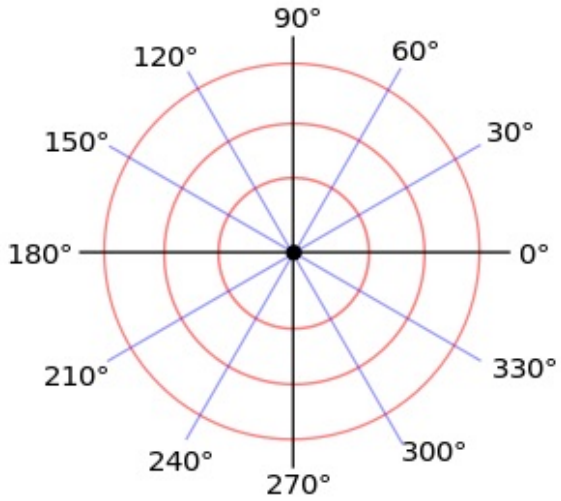
le 4 corrispondono anche alle 16 del pomeriggio
16 è congruo a 4 modulo 12
$16 \equiv 4 \pmod{12}$

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

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



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



$$370 \equiv 10 \pmod{360}$$
$$750 \equiv 30 \pmod{360}$$
$$-90 \equiv 270 \pmod{360}$$

Possiamo estendere le congruenze ai numeri negativi, ad esempio:

Possiamo estendere le congruenze ai numeri negativi, ad esempio:

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

Possiamo estendere le congruenze ai numeri negativi, ad esempio:

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

A volte è utile ragionare così:

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 ...

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 ...

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

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

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

Congruenza modulo n e Attività I

DEFINIZIONE (congruenza modulo n)

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

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

Si può proporre una attività a partire da un altro orologio come il seguente:

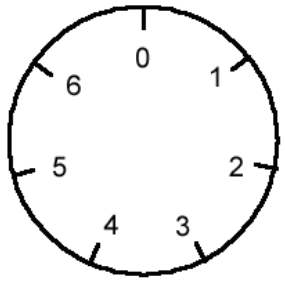
Congruenza modulo n e Attività I

DEFINIZIONE (congruenza modulo n)

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

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

Si può proporre una attività a partire da un altro orologio come il seguente:



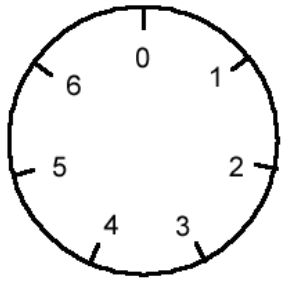
Congruenza modulo n e Attività I

DEFINIZIONE (congruenza modulo n)

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

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

Si può proporre una attività a partire da un altro orologio come il seguente:



Aiutandoti con l'orologio in figura trova un numero b minore di 7 tale che

$$17 \equiv b \pmod{7}$$

b è il resto della divisione $17 : 7$ quindi $17 = \ldots \cdot 7 + \ldots$

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Pertanto, fissato n, si ripartisce l'insieme $\mathbb{Z}$ nelle seguenti classi:

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Pertanto, fissato n, si ripartisce l'insieme $\mathbb{Z}$ nelle seguenti classi:

- $[0]_n$: numeri interi che divisi per n danno come resto 0 (multipli di n);

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Pertanto, fissato n, si ripartisce l'insieme $\mathbb{Z}$ nelle seguenti classi:

- $[0]_n$: numeri interi che divisi per n danno come resto 0 (multipli di n);
- $[1]_n$: numeri interi che divisi per n danno come resto 1;

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Pertanto, fissato n, si ripartisce l'insieme $\mathbb{Z}$ nelle seguenti classi:

- $[0]_n$: numeri interi che divisi per n danno come resto 0 (multipli di n);
- $[1]_n$: numeri interi che divisi per n danno come resto 1;
- ...

Classi resto in $\mathbb{Z}_n$

- $25 \equiv \ldots \pmod 7$, $\quad 25 = \ldots \cdot 7 + \ldots.$
- $-30 \equiv \ldots \pmod 7$, $\quad -30 = \ldots \cdot 7 + \ldots.$

Dagli esempi precedenti possiamo intuire che ogni numero intero a è congruo, modulo n, a un numero compreso tra 0 e $n-1$.
Per determinarlo basta dividere a per n e considerare il resto r. Infatti

$$a \equiv r \pmod n \quad \text{e} \quad 0 \leq r < n$$

Pertanto, fissato n, si ripartisce l'insieme $\mathbb{Z}$ nelle seguenti classi:

- $[0]_n$: numeri interi che divisi per n danno come resto 0 (multipli di n);
- $[1]_n$: numeri interi che divisi per n danno come resto 1;
- ...
- $[n-1]_n$: numeri interi che divisi per n danno come resto $n-1$.

L'insieme di tali classi viene indicato con $\mathbb{Z}_n$ ed è detto **Insieme delle classi resto modulo** n.

L'insieme di tali classi viene indicato con $\mathbb{Z}_n$ ed è detto **Insieme delle classi resto modulo** n.

TEOREMA

La congruenza modulo n è una relazione di equivalenza

L'insieme di tali classi viene indicato con $\mathbb{Z}_n$ ed è detto **Insieme delle classi resto modulo** n.

TEOREMA

La congruenza modulo n è una relazione di equivalenza

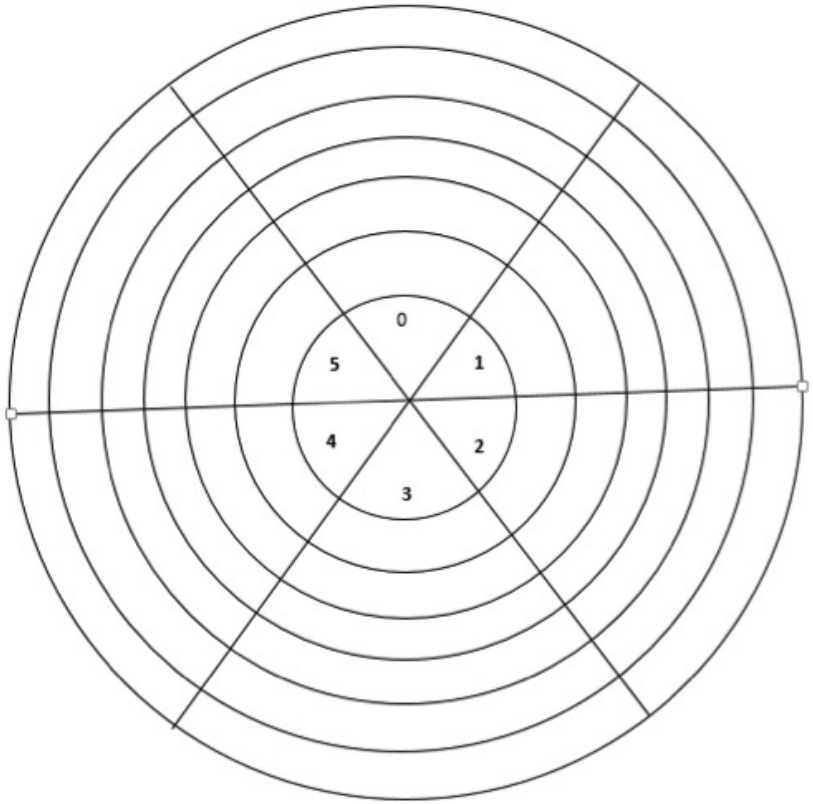
Esercizio Inserisci nelle rispettive classi di $\mathbb{Z}_{10}$ i numeri da 10 a 49

$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$

Attività II

Attività II

Inserisci nelle rispettive classi di $\mathbb{Z}_6$ i numeri da 6 a 41



Operazioni in $\mathbb{Z}_n$

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

Operazioni in $\mathbb{Z}_n$

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

Operazioni in $\mathbb{Z}_n$

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

Operazioni in $\mathbb{Z}_n$

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 $8+35=(8+24)+11=8+11=19$
Considerando vari esempi ci si convince che la somma e la moltiplicazione "rispettano" la congruenza nel senso esplicitato dal seguente teorema.

TEOREMA Siano a, b, c, d numeri interi e n un intero positivo fissato

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

Attività III

- Completa le seguenti tavole additiva e moltiplicativa di $\mathbb{Z}_4$

$+$	0	1	2	3
0				
1				
2				
3				

$\cdot$	0	1	2	3
0				
1				
2				
3				

- Completa le seguenti tavole additiva e moltiplicativa di $\mathbb{Z}_5$

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot$	0	1	2	3	4
0					
1					
2					
3					
4					

- Confrontando le tavole di $\mathbb{Z}_4$ e $\mathbb{Z}_5$ quali differenze noti?

Attività III

- Completa le seguenti tavole additiva e moltiplicativa di $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- Completa le seguenti tavole additiva e moltiplicativa di $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Attività IV

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

Attività IV

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

- $7^2 + (5 \cdot 57) \equiv 40 \pmod{48}$;

Attività IV

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

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

Attività IV

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

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

Attività IV

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!

Attività IV

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 2: pari/dispari

PROBLEMA

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?

La congruenza modulo 2: pari/dispari

PROBLEMA

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?

Scriviamo le tavole per addizione e moltiplicazione modulo 2:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

La congruenza modulo 2: pari/dispari

PROBLEMA

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?

Scriviamo le tavole per addizione e moltiplicazione modulo 2:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Corrispondono alla somma e al prodotto con pari e dispari.

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

NB: Non è possibile scrivere tavole simili per la penultima cifra oppure per la prima cifra.

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

NB: Non è possibile scrivere tavole simili per la penultima cifra oppure per la prima cifra.

ESERCIZIO

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

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

NB: Non è possibile scrivere tavole simili per la penultima cifra oppure per la prima cifra.

ESERCIZIO

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

$$2^{20}$$

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

NB: Non è possibile scrivere tavole simili per la penultima cifra oppure per la prima cifra.

ESERCIZIO

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

$$2^{20} \qquad 17^{17}$$

La congruenza modulo 10: l'ultima cifra

Ogni numero intero positivo è congruo, modulo 10, alla sua ultima cifra, la cifra delle unità. Le tavole per addizione e moltiplicazione descrivono, in questo caso, il comportamento dell'ultima cifra nelle operazioni.

NB: Non è possibile scrivere tavole simili per la penultima cifra oppure per la prima cifra.

ESERCIZIO

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

$$2^{20} \qquad 17^{17} \qquad 2017^{2017}$$

La congruenza modulo 9: la somma delle cifre

Ogni numero intero positivo è congruo, modulo 9, alla somma delle sue cifre.

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:

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:

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

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:

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

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

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:

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

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

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

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:

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

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

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

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

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

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

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

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

possiamo ricavare i criteri di divisibilità:

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

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

possiamo ricavare i criteri di divisibilità:

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

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

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

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

possiamo ricavare i criteri di divisibilità:

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

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

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

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

le congruenze e i criteri di divisibilità

Utilizzando la scrittura polinomiale di un numero intero appena vista

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

possiamo ricavare i criteri di divisibilità:

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

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

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

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

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

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

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

In particolare:

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

In particolare:

prova del 2 il controllo è banale, è bene fare questo controllo, ma non è molto utile, dà un risultato positivo nel 50% dei casi;

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

In particolare:

prova del 2 il controllo è banale, è bene fare questo controllo, ma non è molto utile, dà un risultato positivo nel 50% dei casi;

prova del 10 anche questo controllo è poco interessante, perché ci si limita a controllare l'ultima cifra;

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

In particolare:

prova del 2 il controllo è banale, è bene fare questo controllo, ma non è molto utile, dà un risultato positivo nel 50% dei casi;

prova del 10 anche questo controllo è poco interessante, perché ci si limita a controllare l'ultima cifra;

prova del 9 è semplice e abbastanza utile; tuttavia non segnala due errori relativamente frequenti: scambio di due cifre e errore di incolonnamento nell'esecuzione di una moltiplicazione

le congruenze come strumenti di controllo

Le considerazioni precedenti offrono strumenti di **controllo**
In particolare si tratta del controllo della *correttezza di un'operazione*
condizioni **necessarie ma non sufficienti** per la correttezza del risultato.

In particolare:

prova del 2 il controllo è banale, è bene fare questo controllo, ma non è molto utile, dà un risultato positivo nel 50% dei casi;

prova del 10 anche questo controllo è poco interessante, perché ci si limita a controllare l'ultima cifra;

prova del 9 è semplice e abbastanza utile; tuttavia non segnala due errori relativamente frequenti: scambio di due cifre e errore di incolonnamento nell'esecuzione di una moltiplicazione

prova dell'11 si potrebbe fare ma risulta piuttosto macchinosa

Attività V (Piccolo Teorema di Fermat)

Attività V (Piccolo Teorema di Fermat)

- Sia n un numero naturale da 1 a 4. Calcola, per ogni valore di n, le potenze n^2, n^3, n^4 e n^5 modulo 5. Noti qualche regolarità?

Attività V (Piccolo Teorema di Fermat)

- Sia n un numero naturale da 1 a 4. Calcola, per ogni valore di n, le potenze n^2, n^3, n^4 e n^5 modulo 5. Noti qualche regolarità?
- Considera ora le potenze di 8 e costruisci una tabella come la seguente:

potenze di 8	**potenze di 8 mod 5**
$8^1=8$	3
$8^2=64$	4
$8^3=512$	2
.....	.....

Attività V (Piccolo Teorema di Fermat)

- Sia n un numero naturale da 1 a 4. Calcola, per ogni valore di n, le potenze n^2, n^3, n^4 e n^5 modulo 5. Noti qualche regolarità?
- Considera ora le potenze di 8 e costruisci una tabella come la seguente:

potenze di 8	**potenze di 8 mod 5**
$8^1=8$	3
$8^2=64$	4
$8^3=512$	2
.....	.....

continua la tabella precedente fino alla settima potenza e analizza la seconda colonna. Come puoi esprimere a parole la struttura della seconda colonna?

- costruisci una tabella analoga alla precedente per le potenze di 10 modulo 7

- costruisci una tabella analoga alla precedente per le potenze di 10 modulo 7
- cosa puoi dedurre dai due esempi precedenti? Cosa succede scegliendo altri numeri al posto di 10 e 7? Cerca di enunciare una proprietà generale.

- costruisci una tabella analoga alla precedente per le potenze di 10 modulo 7
- cosa puoi dedurre dai due esempi precedenti? Cosa succede scegliendo altri numeri al posto di 10 e 7? Cerca di enunciare una proprietà generale.

gli esempi visti sono casi particolari del:

- costruisci una tabella analoga alla precedente per le potenze di 10 modulo 7
- cosa puoi dedurre dai due esempi precedenti? Cosa succede scegliendo altri numeri al posto di 10 e 7? Cerca di enunciare una proprietà generale.

gli esempi visti sono casi particolari del:

Piccolo Teorema di Fermat

Se p è primo e a non è multiplo di p allora $a^{p-1} \equiv 1 \pmod{p}$ e quindi $a^p \equiv a \pmod{p}$

- costruisci una tabella analoga alla precedente per le potenze di 10 modulo 7
- cosa puoi dedurre dai due esempi precedenti? Cosa succede scegliendo altri numeri al posto di 10 e 7? Cerca di enunciare una proprietà generale.

gli esempi visti sono casi particolari del:

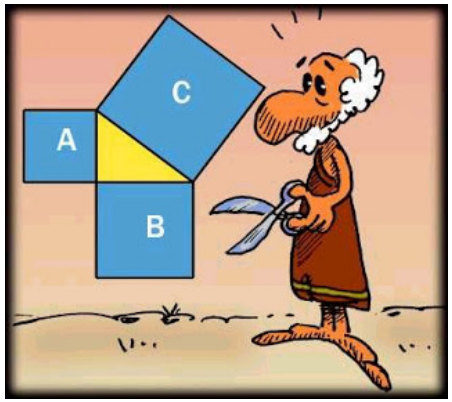
Piccolo Teorema di Fermat

Se p è primo e a non è multiplo di p allora $a^{p-1} \equiv 1 \pmod{p}$ e quindi $a^p \equiv a \pmod{p}$

Per inciso, da quanto visto si deduce che, per ogni numero naturale n, n ed n^5 hanno la stessa cifra delle unità

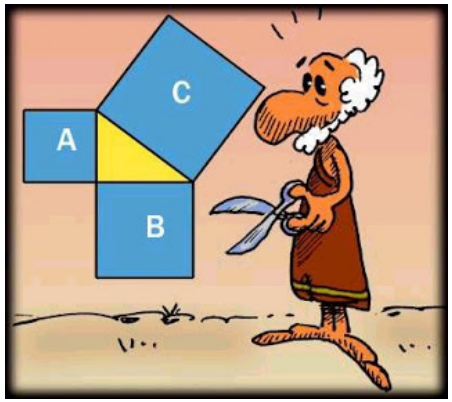
terne pitagoriche modulo 2

Possiamo caratterizzare le terne pitagoriche $a^2 + b^2 = c^2$ in $\mathbb{Z}_n$.



terne pitagoriche modulo 2

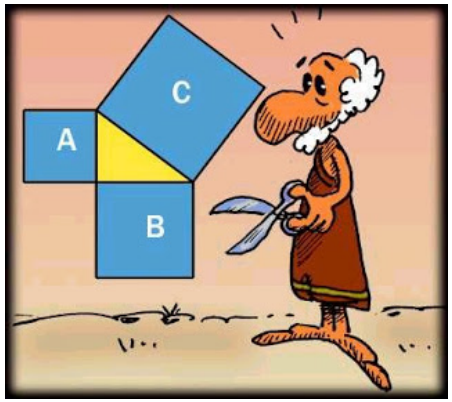
Possiamo caratterizzare le terne pitagoriche $a^2 + b^2 = c^2$ in $\mathbb{Z}_n$.



Ciò fornisce informazioni sui numeri che compongono una terna.

terne pitagoriche modulo 2

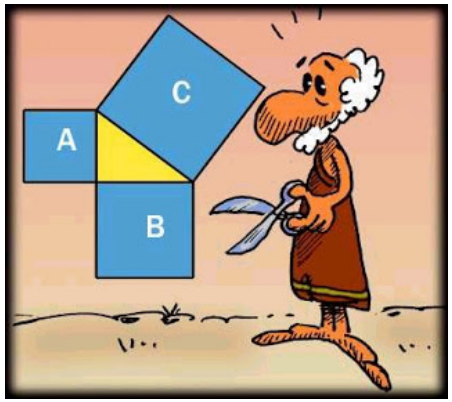
Possiamo caratterizzare le terne pitagoriche $a^2 + b^2 = c^2$ in $\mathbb{Z}_n$.



Ciò fornisce informazioni sui numeri che compongono una terna.
Escludiamo dal nostro studio le terne non primitive.

terne pitagoriche modulo 2

Possiamo caratterizzare le terne pitagoriche $a^2 + b^2 = c^2$ in $\mathbb{Z}_n$.



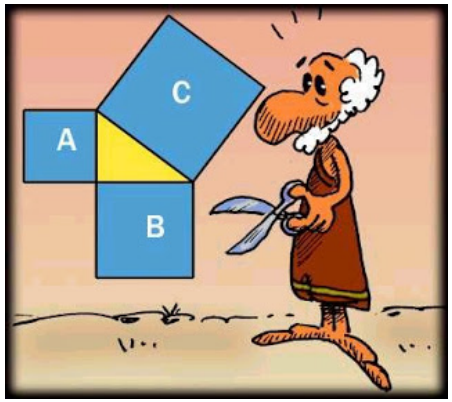
Ciò fornisce informazioni sui numeri che compongono una terna.
Escludiamo dal nostro studio le terne non primitive.
Modulo 2 i quadrati sono

n	0	1
n^2	0	1

dato che la terna (pari, pari, pari) non è primitiva, restano:

terne pitagoriche modulo 2

Possiamo caratterizzare le terne pitagoriche $a^2 + b^2 = c^2$ in $\mathbb{Z}_n$.



Ciò fornisce informazioni sui numeri che compongono una terna.
Escludiamo dal nostro studio le terne non primitive.
Modulo 2 i quadrati sono

n	0	1
n^2	0	1

dato che la terna (pari, pari, pari) non è primitiva, restano:

(pari, dispari, dispari), (dispari, pari, dispari) e (dispari, dispari, pari)

terne pitagoriche modulo 4

Modulo 4 i quadrati sono

n	0	1	2	3
n^2	0	1	0	1

terne pitagoriche modulo 4

Modulo 4 i quadrati sono

n	0	1	2	3
n^2	0	1	0	1

osserviamo che 2 non è un quadrato modulo 4. Quindi le uniche terne pitagoriche sono:

terne pitagoriche modulo 4

Modulo 4 i quadrati sono

n	0	1	2	3
n^2	0	1	0	1

osserviamo che 2 non è un quadrato modulo 4. Quindi le uniche terne pitagoriche sono:

(pari, dispari, dispari), (dispari, pari, dispari).

terne pitagoriche modulo 4

Modulo 4 i quadrati sono

n	0	1	2	3
n^2	0	1	0	1

osserviamo che 2 non è un quadrato modulo 4. Quindi le uniche terne pitagoriche sono:

(pari, dispari, dispari), (dispari, pari, dispari).

quindi possiamo escludere la terna:

(dispari, dispari, pari)

terne pitagoriche modulo 3

Modulo 3 i quadrati sono

terne pitagoriche modulo 3

Modulo 3 i quadrati sono

n	0	1	2
n^2	0	1	1

partiamo da $a^2 + b^2 = c^2$ e consideriamo l'uguaglianza modulo 3. Le uniche possibilità sono:

terne pitagoriche modulo 3

Modulo 3 i quadrati sono

n	0	1	2
n^2	0	1	1

partiamo da $a^2 + b^2 = c^2$ e consideriamo l'uguaglianza modulo 3. Le uniche possibilità sono:

$$0 + 1 = 1 \quad \text{oppure} \quad 1 + 0 = 1$$

quindi

terne pitagoriche modulo 3

Modulo 3 i quadrati sono

n	0	1	2
n^2	0	1	1

partiamo da $a^2 + b^2 = c^2$ e consideriamo l'uguaglianza modulo 3. Le uniche possibilità sono:

$$0 + 1 = 1 \quad \text{oppure} \quad 1 + 0 = 1$$

quindi

un cateto (e uno solo) deve essere multiplo di 3.

terne pitagoriche modulo 5

Modulo 5 i quadrati sono

terne pitagoriche modulo 5

Modulo 5 i quadrati sono

n	0	1	2	3	4
n^2	0	1	4	4	1

consideriamo l'uguaglianza $a^2 + b^2 = c^2$ modulo 5. Le uniche possibilità (a meno dell'ordine) sono:

terne pitagoriche modulo 5

Modulo 5 i quadrati sono

n	0	1	2	3	4
n^2	0	1	4	4	1

consideriamo l'uguaglianza $a^2 + b^2 = c^2$ modulo 5. Le uniche possibilità (a meno dell'ordine) sono:

$$0 + 1 = 1 \quad \text{oppure} \quad 0 + 4 = 4 \quad \text{oppure} \quad 1 + 4 = 0$$

quindi

terne pitagoriche modulo 5

Modulo 5 i quadrati sono

n	0	1	2	3	4
n^2	0	1	4	4	1

consideriamo l'uguaglianza $a^2 + b^2 = c^2$ modulo 5. Le uniche possibilità (a meno dell'ordine) sono:

$$0 + 1 = 1 \quad \text{oppure} \quad 0 + 4 = 4 \quad \text{oppure} \quad 1 + 4 = 0$$

quindi

in ogni terna c'è almeno un multiplo di 5 che può essere anche l'ipotenusa (0+1=1, 1+4=0)

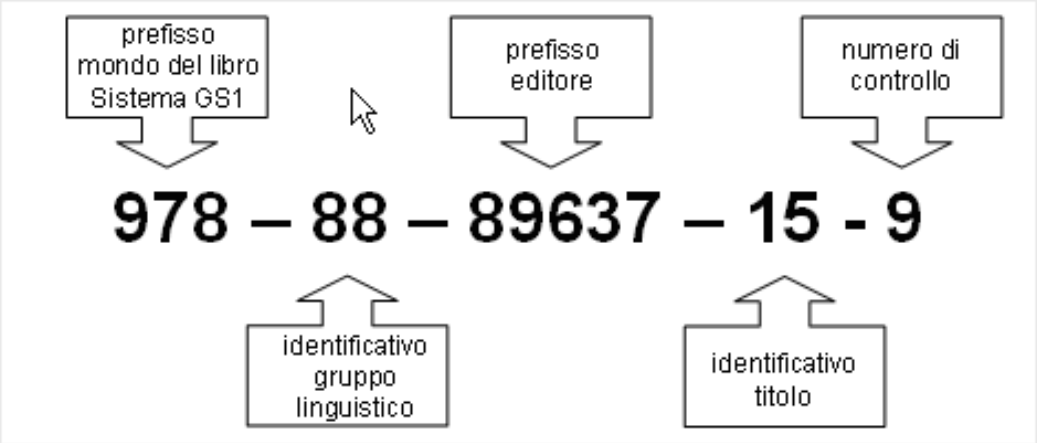
Il codice ISBN

Nel retro di copertina di ogni libro c'è un codice a barre e sotto di esso un codice di 13 cifre, si chiama codice ISBN.

Il codice ISBN

Nel retro di copertina di ogni libro c'è un codice a barre e sotto di esso un codice di 13 cifre, si chiama codice ISBN.

L'ISBN - International Standard Book Number - un numero che identifica a livello internazionale in modo univoco e duraturo un titolo o una edizione di un titolo di un determinato editore



La cifra di controllo

Le prime 12 cifre dell'ISBN contengono informazioni sul prodotto mentre l'ultima è una **cifra di controllo**.

La cifra di controllo

Le prime 12 cifre dell'ISBN contengono informazioni sul prodotto mentre l'ultima è una **cifra di controllo**.

Serve a controllare se il codice è esatto

La cifra di controllo

Le prime 12 cifre dell'ISBN contengono informazioni sul prodotto mentre l'ultima è una **cifra di controllo**.

Serve a controllare se il codice è esatto
Come funziona?

La cifra di controllo

Le prime 12 cifre dell'ISBN contengono informazioni sul prodotto mentre l'ultima è una **cifra di controllo**.

Serve a controllare se il codice è esatto
Come funziona?

Siano $d_1, d_2, ..., d_{13}$ le cifre del codice ISBN di un libro

Se le cifre del codice ISBN sono corrette allora il numero:

$$d_1 + 3 \cdot d_2 + d_3 + 3 \cdot d_4 + d_5 + ... + 3 \cdot d_{12} + d_{13}$$

è multiplo di 10

La cifra di controllo

Le prime 12 cifre dell'ISBN contengono informazioni sul prodotto mentre l'ultima è una **cifra di controllo**.

Serve a controllare se il codice è esatto
Come funziona?

Siano $d_1, d_2, ..., d_{13}$ le cifre del codice ISBN di un libro

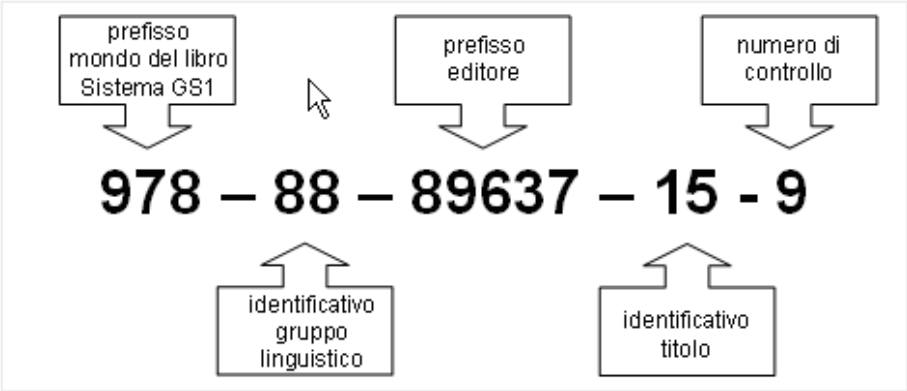
Se le cifre del codice ISBN sono corrette allora il numero:

$$d_1 + 3 \cdot d_2 + d_3 + 3 \cdot d_4 + d_5 + ... + 3 \cdot d_{12} + d_{13}$$

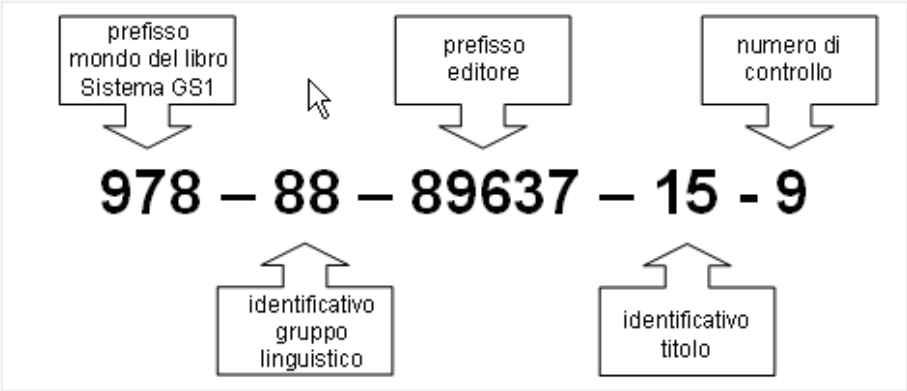
è multiplo di 10

L'affermazione precedente può essere rienunciata in termini di congruenze modulo 10.

Verifichiamo l'ISBN precedente utilizzando l'aritmetica modulare per velocizzare i calcoli:



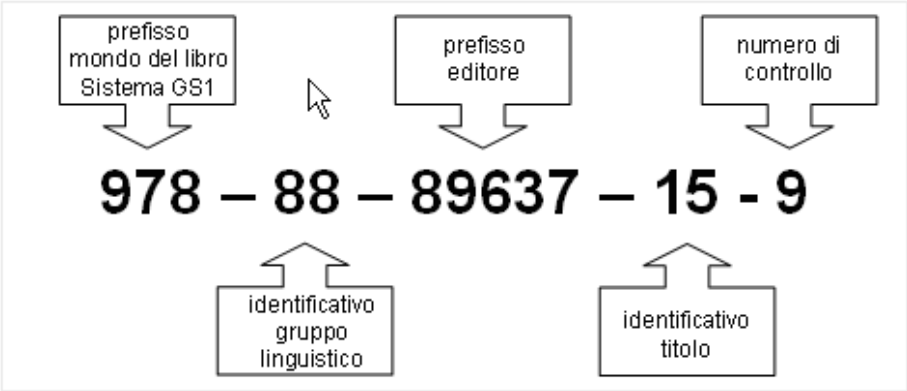
Verifichiamo l'ISBN precedente utilizzando l'aritmetica modulare per velocizzare i calcoli:



$$9+3\cdot 7+8+3\cdot 8+8+3\cdot 8+9+3\cdot 6+3+3\cdot 7+1+3\cdot 5+9\equiv$$

$$\equiv \not{9}+\not{1}+\not{8}+\not{4}+\not{8}+4+\not{9}+\not{8}+\not{3}+1+\not{1}+5+\not{9}\equiv 0 \pmod{10}$$

Verifichiamo l'ISBN precedente utilizzando l'aritmetica modulare per velocizzare i calcoli:



$$9+3\cdot 7+8+3\cdot 8+8+3\cdot 8+9+3\cdot 6+3+3\cdot 7+1+3\cdot 5+9\equiv$$

$$\equiv \not{9}+\not{1}+\not{8}+\not{4}+\not{8}+4+\not{9}+\not{8}+\not{3}+1+\not{1}+5+\not{9}\equiv 0 \pmod{10}$$

NB: La cifra di controllo ci fornisce solo una CONDIZIONE NECESSARIA per la correttezza del codice!

Attività VI

Attività VI

- Prendi tre libri a tua scelta e, utilizzando l'aritmetica modulare (senza calcolatrice), controlla la correttezza del loro codice ISBN

Attività VI

- Prendi tre libri a tua scelta e, utilizzando l'aritmetica modulare (senza calcolatrice), controlla la correttezza del loro codice ISBN
- Quale dei seguenti codici ISBN è corretto?

9788860220587 97888806320587

9788806220687 9788806220587

Attività VI

- Prendi tre libri a tua scelta e, utilizzando l'aritmetica modulare (senza calcolatrice), controlla la correttezza del loro codice ISBN
- Quale dei seguenti codici ISBN è corretto?

9788860220587 97888806320587

9788806220687 9788806220587

- Nei seguenti codici ISBN manca una cifra: trova la cifra mancante:

978880816204... 97888477...2810 97888045989...7

Attività VII

Un amico ti ha scritto su un foglietto di carta l'ISBN di un libro che vuole consigliarti, purtroppo nella sua scrittura i 7 si confondono con gli 1. Se il codice che leggi sul foglietto è

3908730681238

è possibile risolvere l'ambiguità di scrittura? In caso affermativo determina l'ISBN corretto altrimenti spiega perché ciò non è possibile.

Riflessione I

Riflessione I

- Secondo te il metodo che abbiamo analizzato permette di individuare ogni errore di trascrizione di un ISBN?

Riflessione I

- Secondo te il metodo che abbiamo analizzato permette di individuare ogni errore di trascrizione di un ISBN?
- Se così non fosse, fai un esempio di errore che non può essere individuato.

Riflessione II

Perché, a tuo avviso, nel codice ISBN si moltiplicano per 3 le cifre di posto pari e solo quelle?

Riflessione II

Perché, a tuo avviso, nel codice ISBN si moltiplicano per 3 le cifre di posto pari e solo quelle?
Suggerimento: *prova a scambiare due cifre tra le prime 12*

Riflessione III

Perché, a tuo avviso, si usa il 3 nel controllo del codice ISBN e non un altro numero come, ad esempio, il 5?

Riflessione III

Perché, a tuo avviso, si usa il 3 nel controllo del codice ISBN e non un altro numero come, ad esempio, il 5?
Suggerimento: *moltiplica tutti i numeri da 0 a 9 per 3 e scrivi i risultati modulo 10. Fai la stessa cosa con 5. Che differenze noti?*. Ci sono altri numeri che potrebbero essere usati al posto del 3?

Esplorazioni

Esplorazioni

1. Puoi pensare ad un altro metodo, sempre basato sull'aritmetica modulare, che consenta di individuare anche gli errori che hai individuato nella riflessione I?
   Inventa un nuovo metodo per trovare la cifra di controllo!

Esplorazioni

1. Puoi pensare ad un altro metodo, sempre basato sull'aritmetica modulare, che consenta di individuare anche gli errori che hai individuato nella riflessione I?
   Inventa un nuovo metodo per trovare la cifra di controllo!
2. Anche nel Codice Fiscale l'ultima cifra è di controllo, cerca in rete e scopri come funziona!