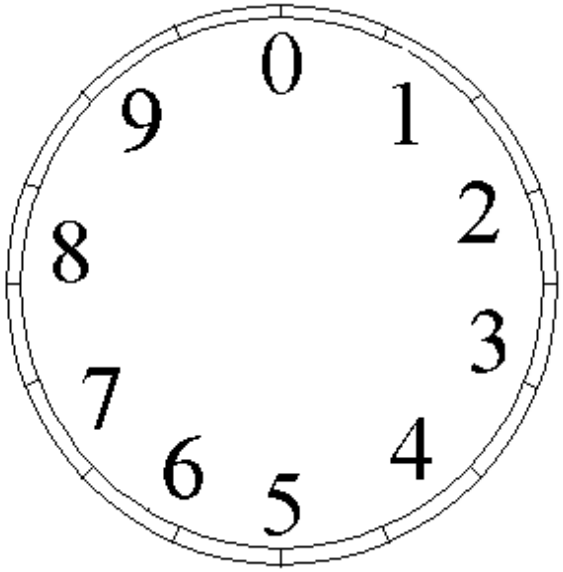
Istituto Statale 'Biagio Pascal'
Istituto Tecnico Tecnologico – Liceo Scientifico
Via Brembio,97- 00188 - Via dei Robilant,2 - 00194 – Roma
Centralino: 06-12112-4205 via Brembio - 06-12112-4225 Via dei Robilant
Codice meccanografico RMTF330002 C.F. 97046890584 Web: www.pascalroma.edu.it
Email: RMTF330002@istruzione.it Pec: RMTF330002@pec.istruzione.it

Liceo Matematico

U.D. 4

Aritmetica modulare e crittografia



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Obiettivi formativi

- Correttezza nel ragionamento

Obiettivi didattici

- Saper scrivere un numero con le congruenze modulo b
- Saper eseguire le operazioni in Z. Tabelle
- Saper riconoscere anelli e campi
- Saper ripetere semplici dimostrazioni
- Saper criptare e decriptare semplici messaggi con i cifrari studiati

Prerequisiti

- Operazioni con i numeri naturali

Materiale

- Cartoncini per creare il cifrario di Cesare e la tabella di Vigenere
- Schede di esercitazione e verifica

Esperienza

- Aritmetica modulare - **Scheda n°1:** riconoscere le congruenze sia per i numeri positivi che negativi
- La relazione di congruenza mod n in Z.
- Classi di resti modulo n. - **Scheda n°2**: costruire tabelle di classi resto
- Operazioni di somma e di prodotto in Zn. Gruppi, anelli e campi. - **Scheda n°3**: costruire somma, prodotto, inverso e reciproco in Zn con n primo e non. **Scheda n°4** Nuovi oggetti e nuove operazioni
- Crittografia. Cifrario di Cesare - **Scheda n°5** cifrario di Cesare additivo e moltiplicativo - **Scheda n°6** cifrario di Cesare con cerchi concentrici
- Cifrario di Vigenere - **Scheda n°7** uso della tabella di Vigenere

Verifica

- Compilare le tabelle vuote
- Ripetere semplici dimostrazioni
- Saper criptare e decriptare messaggi con le tecniche illustrate

Tempi: 8 ore (10 ore)

1. Aritmetica modulare

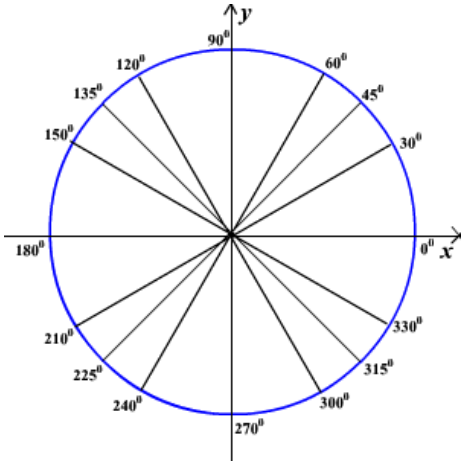
L'aritmetica ordinaria opera su insiemi infiniti di numeri: l'insieme N dei numeri naturali N={0,1,2,3,4...} e quello dei relativi Z={0,±1,±2,±3,±4...}.

Nella realtà però si ha spesso a che fare con situazioni nelle quali i numeri possibili sono finiti; l'orologio ha solo 12 o 24 ore.

Si definisce allora *aritmetica finita* un'aritmetica che opera su un insieme limitato di numeri. Si dice anche aritmetica *modulare* o *circolare*, in quanto una volta raggiunto l'ultimo numero si ricomincia dal primo.

Consideriamo l'insieme delle ore di un orologio analogico. Queste sono 12 (modulo) e vanno da 0 a 11. Noi sappiamo che le 4 corrisponde anche alle 16 del pomeriggio, in gergo matematico si dice che "16 è congruo a 4 modulo 12" e si scrive 16≡4 modulo 2.

Analogamente, consideriamo i gradi di un angolo giro, possiamo dire che 370≡10 modulo 360 o che 750≡30 modulo 360.



E’ possibile dare la congruità anche a numeri negativi, ad esempio per calcolare -19 modulo 12, dobbiamo sommare i multipli del modulo invece che toglierli, fino ad ottenere il numero positivo: -19+12*2=5, quindi -19≡5 modulo 12.

Come calcolare il modulo.

Per sapere che cosa è congruo ad a (mod. n), dividere a per n e prelevare il resto r. In sostanza si dice che a≡r (mod n) se r è il resto della divisione a/n.

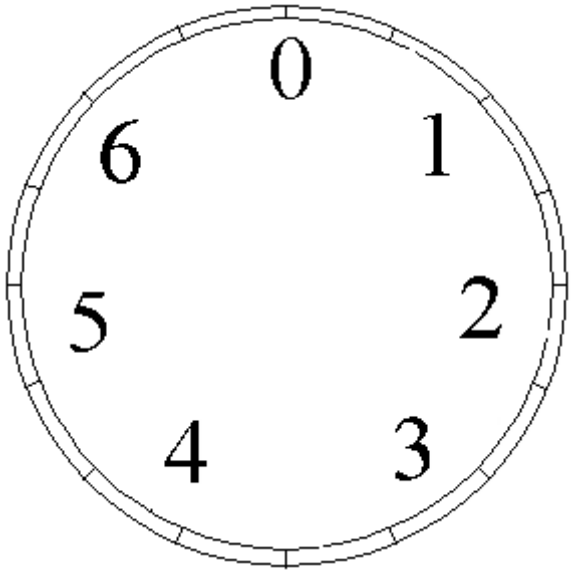
Ricapitoliamo: la relazione di congruenza mod n in Z.

Definizione: Siano a, b ∈Z ed n un intero n > 1. Si dice “a è congruo a b” modulon e si scrive

$$a \equiv b \ (mod\ n) \text{ se } \exists h \in Z \text{ tale che } a - b = hn$$

SCHEDA N° 1 – ARITMETICA MODULARE

Completa:



❖ 16 ≡….. mod 7

Conta sull'orologio e completa al posto dei puntini.Ora fai la divisione per 7 e completa al posto dei puntini.

16 = …..* 7 + …..

❖ 30 ≡….. mod 7

Conta sull'orologio e completa al posto dei puntini.Ora fai la divisione per 7 e completa al posto dei puntini.

30 = …..* 7 + …..

❖ 35 ≡….. mod 7

Conta sull'orologio e completa al posto dei puntini. Ora fai la divisione per 7 e completa al posto dei puntini.

35 =…..* 7 …..

❖ -11 ≡….. mod 7

Conta sull'orologio e completa al posto dei puntini.Ora fai la divisione per 7 e completa al posto dei puntini.

-11+ …. * …. = …..

❖ -24 ≡….. mod 7

Conta sull'orologio ecompleta al posto dei puntini. Ora fai la divisione per 7 e completa al posto dei puntini.

-24+ …. * …. = …..

❖ -30 ≡….. mod 7

Conta sull'orologio completa al posto dei puntini. Ora fai la divisione per 7 e completa al posto dei puntini.

-30+ …. * …. = …..

2. La relazione di congruenza mod n in Z.

La relazione di congruenza (mod n) é una relazione di equivalenza in Z.

Dimostrazione.

1. **Proprietà riflessiva**: $\forall a \in Z$ è $a \equiv a \pmod n$: infatti $a - a = 0 \cdot n$.

2. **Proprietà simmetrica**: sia $a \equiv b \pmod n \Rightarrow \exists\ h \in Z$ tale che $a - b = h \cdot n$;
ma è anche $b - a = (-h) \cdot n$, $(-h) \in Z$ quindi $b \equiv a \pmod n$.

3. **Proprietà transitiva**: $a \equiv b \pmod n \Rightarrow \exists h \in Z$ tale che $a - b = h \cdot n$;
$b \equiv c \pmod n \Rightarrow \exists k \in Z$ tale che $b - c = k \cdot n$.

Sommando membro a membro si ottiene $a - c = (h + k) \cdot n$ da cui segue che $a \equiv c \pmod n$.

3. Classi di resti modulo n.

Fissato $n > 1$, l'insieme Z può essere ripartito in classi di congruenza (includendo in una stessa classe tutti e soli gli $z \in Z$ a due a due congrui tra loro modulo n).

La classe di congruenza individuata da x è:
$[x]_n = \{x + hn |\ h \in Z\} = \{y |\ y \equiv x \pmod n\}$.

Fissato $n > 1$, si hanno esattamente **n classi di equivalenza distinte**, che possono essere rappresentate dai numeri $0, 1, \ldots, n-1$.

L'insieme di queste classi di equivalenza è indicato con il simbolo Zn e viene usualmente chiamato "insieme delle classi di resti modulo n".

Si ha quindi
$Zn = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

SCHEDA N° 2 – ARITMETICA MODULARE

Inserisci nelle rispettive classi di equivalenza i numeri da 7 a 48

$Z_7 = \{[0]_7, [1]_7, \ldots, [n-1]_7\}$

$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$

Inserisci nelle rispettive classi di equivalenza i numeri da 10 a 49

$Z_{10} = \{[0]_{10}, [1]_{10}, \ldots, [n-1]_{10}\}$

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

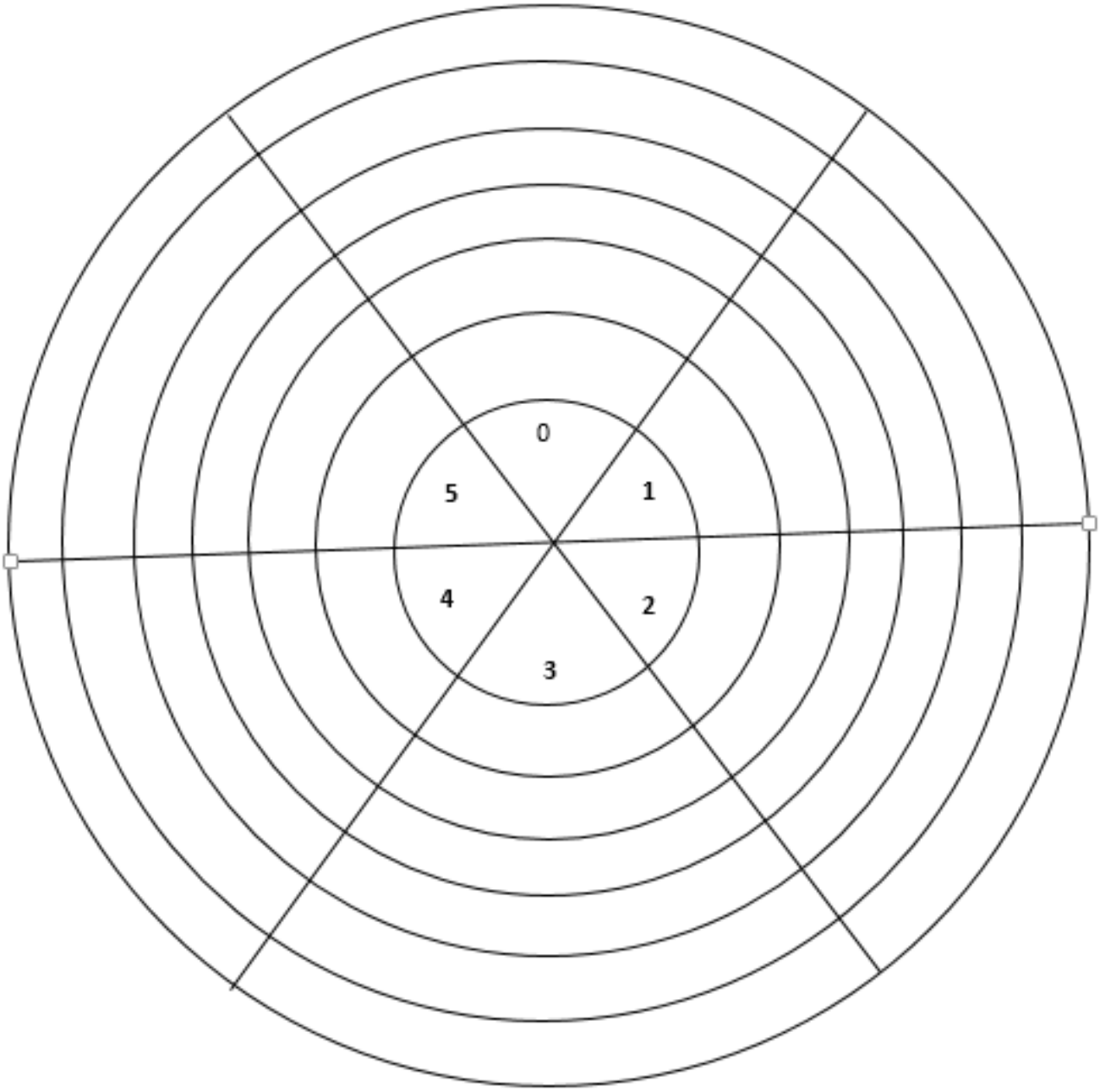
Inserisci nelle rispettive classi di equivalenza i numeri da 13 a 64

$Z_{13} = \{[0]_{13}, [1]_{13}, \ldots, [n-1]_{13}\}$

$[0]_{13}$	$[1]_{13}$	$[2]_{13}$	$[3]_{13}$	$[4]_{13}$	$[5]_{13}$	$[6]_{13}$	$[7]_{13}$	$[8]_{13}$	$[9]_{13}$	$[10]_{13}$	$[11]_{13}$	$[12]_{13}$

Inserisci nelle rispettive classi di equivalenza i numeri da 6 a 41

$Z_6 = \{[0]_7, [1]_7, \ldots, [n-1]_6\}$



4.Operazioni di somma e di prodotto in Z_n. Gruppi, anelli e campi.

Osserviamo ora i legami che sussistono tra le operazioni di somma e di prodotto definiti in Z ela relazione di congruenza modulo n.

La relazione di congruenza (mod n) è compatibile con le operazioni di somma e di prodotto di Z, cioè se a, b $\in$Z da $a \equiv b \pmod n$ e $c \equiv d \pmod n$ segue
$a + c \equiv b + d \pmod n$
$a \cdot c \equiv b \cdot d \pmod n$.

Dimostrazione.
Poichè $a \equiv b \pmod n$ e $c \equiv d \pmod n$ esistono h, k $\in$Z tali che:
$a - b = hn$, $c - d = kn$.
Da qui, sommando membro a membro otteniamo:
$(a - b) + (c - d) = hn + kn$
cioè $(a + c) - (b + d) = (h + k)n$, da cui segue $a + c \equiv b + d \pmod n$.
Analogamente, moltiplicando membro a membro, si ottiene che:
$ac = (b + hn)(d + kn) = bd + (bk + hd + hk)n \Rightarrow ac \equiv bd \pmod n$.

Proviamo a costruire la somma in Z_7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Proviamo a vedere se:

Esiste l'elemento neutro e il simmetrico.(nell'ordine prima il neutro poi il simmetrico)
L'elemento neutro è quell'elemento u tale che a + u = u + a, nel nostro caso è 0
L'elemento simmetrico (o in questo caso opposto) a+ (-a) = (-a) +a = u

Dalla tavola della somma si vede che l'elemento neutro è lo 0 e che , per esempio, il simmetrico di 4 è 3 perché 4+3 = 0 (elemento neutro)

a	0	1	2	3	4	5	6
-a	0	6	5	4	3	2	1

Vale la **proprietà associativa**, perché vale in Z, infatti:

a + (b+c) = (a+b) + c

Definizione: un **gruppo** G è un insieme fornito di una operazione + :
per cui valgono le seguenti proprietà:

Associatività: per ogni x; y; z ∈G
x + (y + z) = (x +y) + z:
Elemento neutro: Esiste un elemento u∈G tale che per ogni x ∈G
x + u = u+ x = x:(nella somma è lo 0)
simmetrico (in questo caso opposto): Per ogni x ∈G esiste y∈G tale che
x+y=y+x= u

Se in aggiunta vale la proprietà
Commutatività: per ogni x; y ∈G
x + y = y + x:
il gruppo G si dice **commutativo** oppure **abeliano**.

Questo fa sì che Zn sia un **gruppo additivo**

Proviamo a costruire il prodotto "∗"in Z_7

∗	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	***1***	2	3	4	5	6
2	0	2	4	6	***1***	3	5
3	0	3	6	2	5	***1***	4
4	0	4	***1***	5	2	6	3
5	0	5	3	***1***	6	4	2
6	0	6	5	4	3	2	***1***

Abbiamo già visto che Z_7 è un **gruppo abeliano** per la somma, osserviamo che vale la *

proprietà associativa per il prodotto (perché vale in Z);

esiste **l'elemento neutro** per il prodotto $1 * x = x * 1 = x$ (identità)

Vale la **proprietà distributiva**(perché vale in Z)

Allora Z_7 è un anello (in generale Zn)

Definizione: Un anello **R** è un insieme fornito di due operazioni, **addizione** "+" e **moltiplicazione** "$*$", che soddisfano le seguenti proprietà:

rispetto alla prima operazione "+"
(Gruppo additivo) L'insieme **(R; +) è un gruppo abeliano**.

Rispetto alla seconda operazione "$*$"

Associatività: per ogni x; y; z $\in$R
$(x * y) * z = x * (y * z)$;
Elemento neutro: esiste un elemento $\in$R,(nel prodotto è 1), con la proprietà che per ogni x $\in$R
$1 * x = x * 1 = x$;
Distributività: per ogni x; y; z $\in$R
$x * (y + z) = x * y + x * z$;
$(y + z) * x = y * x + z * x$;

Se in aggiunta vale la proprietà
Commutatività: per ogni x, y $\in$R
$x * y = y * x$;
l'anello R si dice **commutativo**.

Se l'anello è commutativo ed esiste il simmetrico **moltiplicativo:**
per ogni x $\in$R, x $\neq$ 0 esiste $x^{-1} \in$R tale che
$x * x^{-1} = x^{-1} * x = 1$;
l'anello R si dice un CAMPO.

/

Proviamo a costruire il prodotto "$*$"in Z_6

$*$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

L'elemento neutro è 1, ma non ho il simmetrico per ogni numero. Infatti 2, 3,4 non hanno il simmetrico (nel prodotto si chiama reciproco) cioè non esiste un numero in Z_6 che moltiplicato per 2 o per 3, o 4 dia come risultato 1.
Quindi Z_6 non è un campo. Esistono i divisori dello zero.

Proposizione:
Sia n un intero positivo.
L'anello Zn è un campo se e soltanto se n è un numero primo.

SCHEDA N° 3 – ARITMETICA MODULARE

Completa la tabella della somma in $Z_{11.}$

+	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Trova l'opposto.

a	0	1	2	3	4	5	6	7	8	9	10
-a											

Z_{11} è un gruppo? E' abeliano?

Completa la tabella del prodotto in Z_{11}

*	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Trova il reciproco.

a	0	1	2	3	4	5	6	7	8	9	10
a^{-1}											

Quali proprietà valgono?

Deduciamo:

SCHEDA N° 4 – **Nuovi oggetti e nuove operazioni**

Nuova operazione:

Nell'insieme Z definiamo l'operazione $\oplus$ così: $a \oplus b = a + b + 7$

es: $15 \oplus 12 = 15 + 12 + 7 = 34$

calcola : $5 \oplus 21 =$_____=_____

$(15 \oplus 12) \oplus 4 =$_____ $15 \oplus (12 \oplus 4) =$ _____

vale la proprietà associativa?

Prova anche se $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

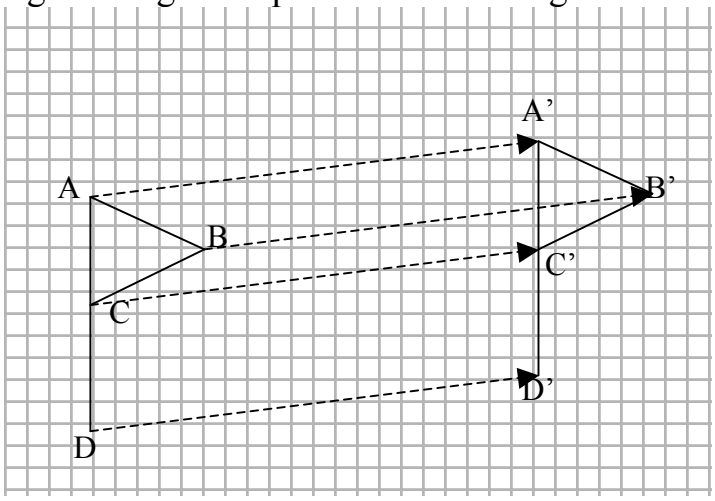
Esiste in Z un numero *u* tale che $3 \oplus u = 3$? e $8 \oplus u = 8$? è lo stesso?

Trova anche il numero *s*tale che $3 \oplus s = u$, e $21 \oplus s = u$

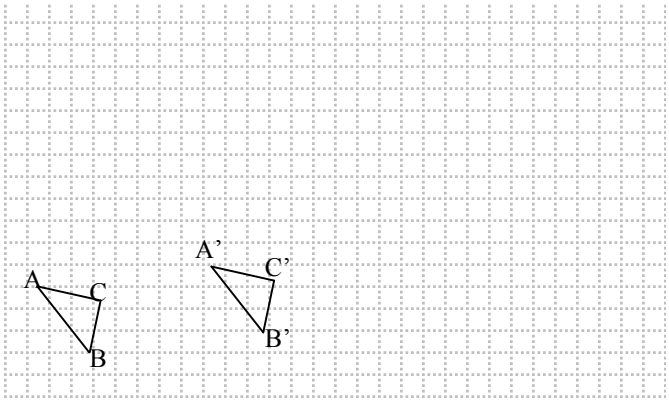
Cosa deduciamo?

Nuovi oggetti e nuove operazioni

La definizione di gruppo si può applicare anche ad oggetti che non sono numeri.
Consideriamo per esempio le traslazioni.
Possiamo considerare le traslazioni come "spostamenti" di una figura: tutti i punti della figura vengono "spostati" in modo uguale.



Le "frecce" indicano lo spostamento e sono tutte uguali.
Nel nostro caso la figura è stata spostata di 27 verso destra e 3 verso l'alto.
La coppia, ordinata, (27; 3) indica lo "spostamento".
La freccia AA' si chiama vettore
E' stata fatta una traslazione $\vec{t}(27; 3)$



Il triangolo ABC è stato traslato nella posizione A'B'C'. Quali sono le componenti del vettore di traslazione ?

$\vec{t}(\_\_; \_\_\_)$

Trasla ora il triangolo A'B'C' secondo il vettore $\vec{s}(10; 5)$. Ottieni il triangolo A"B"C". Disegnalo.

Puoi fare una unica traslazione, $\vec{w}$, da ABC ad A"B"C"? _____

Quali sono le componenti del vettore $\vec{w}$?_____

Confronta le componenti di $\vec{w}$ con quelle di $\vec{t}$ e $\vec{s}$.

Cosa puoi notare? _____

Definiamo la "composizione" di due traslazioni come la "somma" delle componenti dei due vettori di traslazione

$$Se\ \vec{t}(a; b) e\ \vec{s}(c; d)\ allora\ \ \vec{t} \oplus \vec{s} = \vec{w}\ con\ \vec{w}(a + c; b + d)$$

Verifica se l'insieme delle traslazioni con l'operazione "somma" definita prima è un **gruppo**.
E' **associativa**? Date tre traslazioni $\vec{t}, \vec{s}, \vec{z}$ vale $\left(\vec{t} \oplus \vec{s}\right) \oplus \vec{z} = \vec{t} \oplus (\vec{s} \oplus \vec{z})$?

Prova con tre vettori a tua scelta._____

_____

Esiste l'**elemento neutro? (**Una traslazione che lascia immutata la posizione della figura)_____ Se sì, quale è il vettore di traslazione?_____

Esiste la traslazione **simmetrica** rispetto all'operazione di somma?(Quella traslazione che composta ad un'altra mi da' le componenti dell'elemento neutro che hai indicato prima)

_____

_____

_____

Ed infine è **abeliano**? _____
fai un esempio_____

_____

5. Crittografia. Cifrario di Cesare

Esistono particolari fenomeni come quelli temporali che hanno una certa "ciclicità".
Ad esempio: Ore del giorno; Giorni della settimana; Note musicali.

Possiamo pensare alle lettere dell'alfabeto in maniera ciclica con la congruenza modulo 21

La crittografia come tecnica per celare un messaggio esiste fin da tempi antichissimi: i primi rudimentali messaggi cifrati sembra siano contenuti già in alcuni geroglifici egizi della tomba di Knumotete II, risalente al 1900 a.C.

In Grecia gli Spartani usavano intorno al 400 a.C. **la scitala lacedemonica, un bastone verticale su cui erano incisi in ordine le lettere dell'alfabeto. Avvolgendoci sopra un papiro e scrivendo il messaggio verticalmente si aveva il testo trasposto sul papiro: solo riavvolgendolo su un bastone di diametro identico al precedente si poteva ricostruire senza sforzi il messaggio originale.**

Quasi dello stesso periodo sono i primi cifrari ebraici, di cui il più noto è senz'altro il **codice di Atbash, dove si aveva una semplice sostituzione della prima lettera dell'alfabeto con l'ultima, poi della seconda con la penultima, e così via.**

Un altro famosissimo **cifrario storico è quello di Cesare**, che è stato usato per diversi secoli fino all'Alto Medioevo. **In questo cifrario, la sostituzione delle lettere avviene l'uso di un secondo alfabeto costruito partendo da quello in chiaro con le lettere spostate di un certo intervallo numerico prefissato** (intervallo che rappresenta quindi la **chiave**).
Cesare utilizzava uno spostamento di 3 locazioni.
Ecco quindi il nostro alfabeto italiano e quello creato con i 3 spostamenti utilizzati da Cesare:
A B C D E F G H I L M N O P Q R S T U V Z
D E F G H I L M N O P Q R S T U V Z A B C
Usando questo cifrario la parola CIAO diventa FNDR (C->F, I->N, A->D, O->R).

Ovviamente la **robustezza di questo cifrario è molto bassa** ma per l'epoca rappresentava senz'altro un buon metodo per far giungere ai propri comandanti i messaggi sulle manovre militari senza che il nemico potesse decifrarli in caso fosse riuscito a metter mano ai testi.

Può essere utile utilizzare la seguente tabella:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Sia *b* la chiave e*a* il messaggio (un numero ad esempio, oppure il numero associato ad una lettera). La funzione di criptazione è definita come:

$$c(a) := a + b \bmod m.$$ *nel nostro alfabeto m=21*

Per comprendere il messaggio devo fare l'operazione di decriptazione, quindi creare una funzione d(c(a))=a.
Usando il messaggio CIAO con la chiave di Cesare (3) diventato FNDR, per decriptarlo devo "spostare" tutte le lettere " in avanti " di ____ (chiave di decriptazione) in modo tale da riottenere la lettera di partenza . Se b è la chiave di decriptazione e b' quella di decriptazione si deve avere b+b'=0(mod m) cioè nessuno spostamento quindi messaggio originale, quindi b'=m-b

Si potrebbe provare a rendere il cifrario di Cesare più efficace utilizzando il prodotto, cioè la funzione di criptazione sarà c(a) := a · b mod m.

SCHEDA N° 5 – CRITTOGRAFIA

Criptare il vostro nome e cognome con il cifrario di Cesare con chiave 5 e alfabeto a 26 caratteri

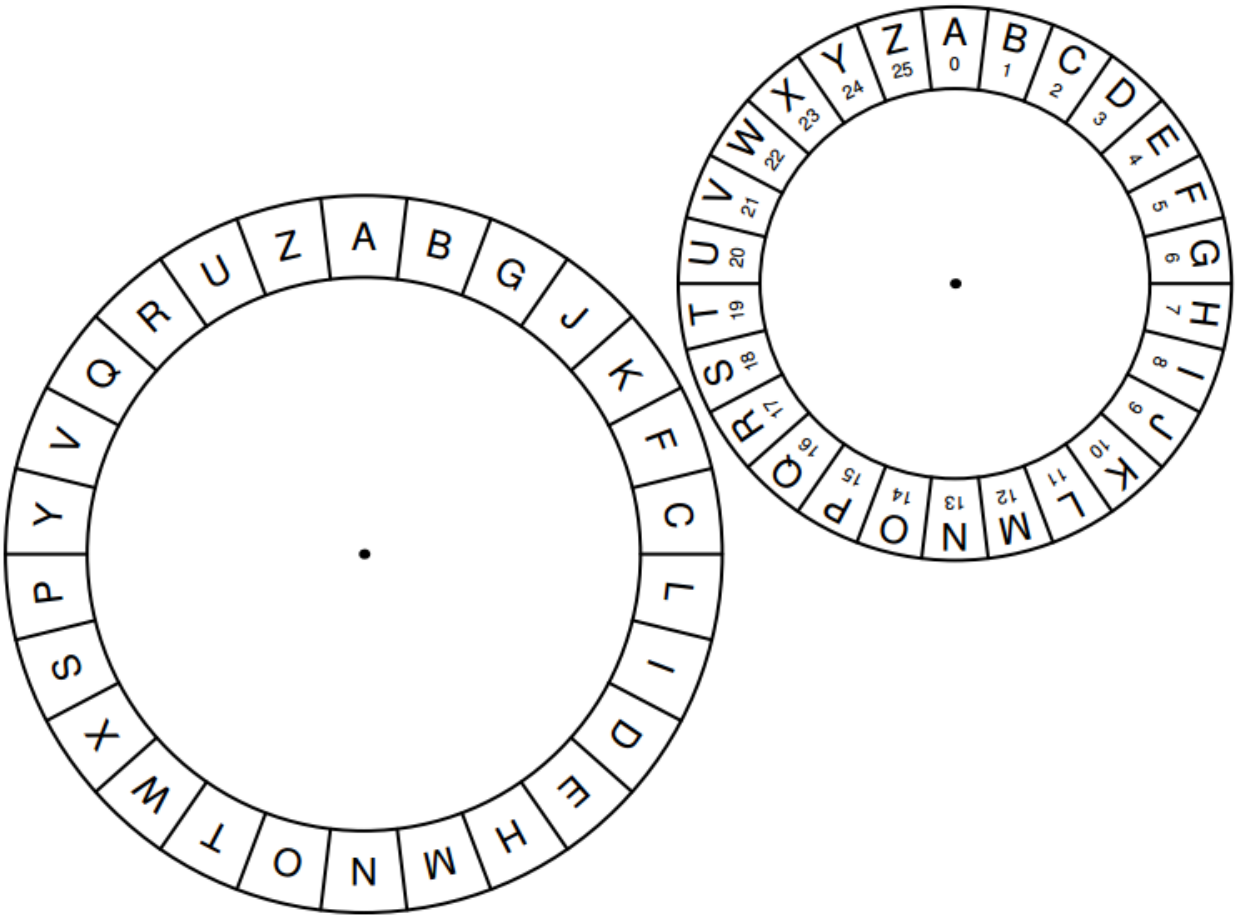
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Criptare il vostro nome e cognome con il cifrario di Cesare, con il metodo del prodotto, con chiave 5 e alfabeto a 26 caratteri

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

SCHEDA N° 6 – CRITTOGRAFIA

Costruisci uno strumento per criptare e decriptare i messaggi ritagliando i cerchi seguenti e fissandoli con un fermacampione al centro



Inserisci un testo nelle righe seguenti e in quelle successive in testo criptato:

Testo in chiaro:

Testo criptato:

6. Cifrario di Vigenere.

B. de Vigenere nel XVI secolo, inventò un cifrario che venne considerato inattaccabile per tre secoli. Esso è sostanzialmente un codice Cesare esteso.
Ecco un esempio del suo funzionamento.
Si prenda una parola chiave ad esempio (alfabeto a 21 caratteri):
“MELA” {11, 5, 10, 1} e la frase da criptare, ad esempio:

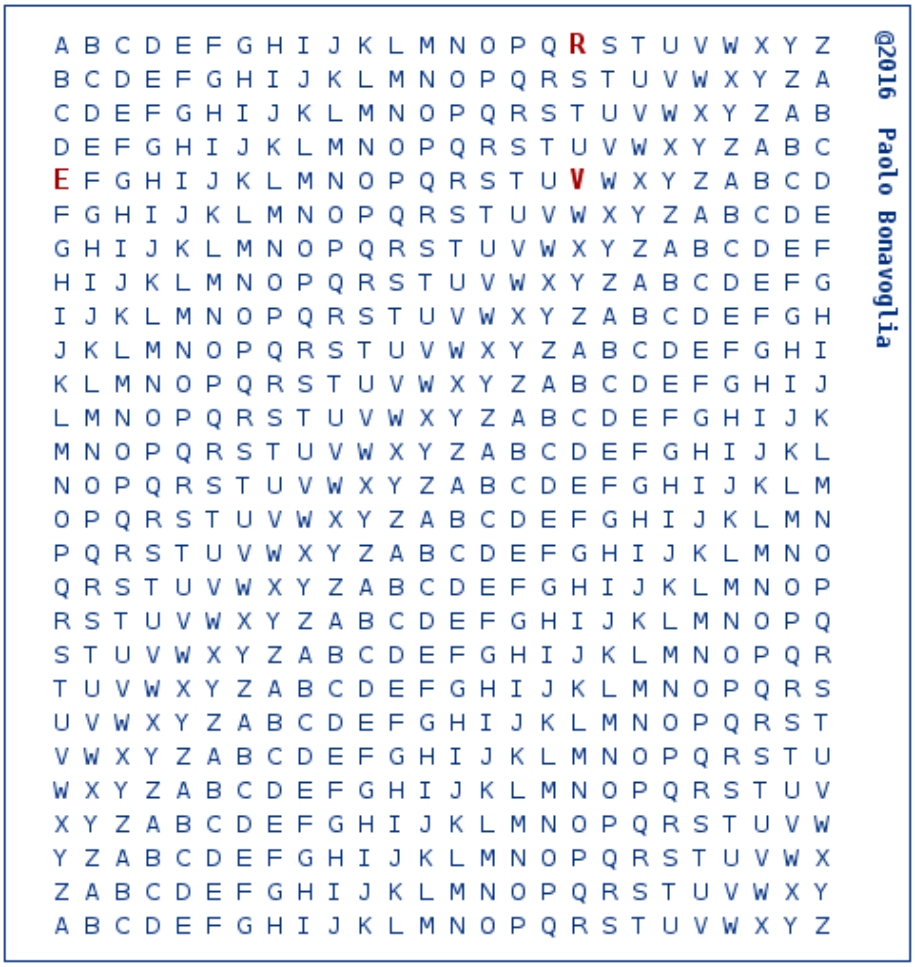
ATTACCAREIMMEDIATAMENTE = {1, 18, 18, 1, 3, 3, 1, 16, 5, 9, 11, 11, 5, 4, 9, 1, 18, 1, 11, 5, 12, 18, 5}. Si sommi la “M” alla prima lettera da criptare, la “E” alla seconda, e così via.
ATTACCAREIMMEDIATAMENTE+MELAMELAMELAMELAMELAMEL=
1, 18, 18, 1, 3, 3, 1, 16, 5, 9, 11, 11, 5, 4, 9, 1, 18, 1, 11, 5, 12, 18, 5 +
11, 5, 10, 1,11, 5, 10, 1,11, 5, 10, 1, 11, 5, 10, 1,11, 5, 10, 1,11, 5, 10,

---

12,23,28,2,14,8,11,17,16,14,21,12,16,9,19,2,29,6,21,6,23,23,15

NBGBPHMSRPZNRIUBHFZFBBQ

Per semplificare questa operazione il Vigénère propose l'uso della seguente **tavola quadrata**, composta da alfabeti ordinati spostati.



Usiamo la tavola con chiave VERME

Volendo ad esempio cifrare la prima R di ARRIVANO si individuerà la colonna della R, quindi si scenderà lungo la colonna fino alla riga corrispondente della corrispondente lettera del VERME (qui E); la lettera trovata all'incrocio è la lettera cifrata (qui V); la seconda R invece sarà cifrata con la lettera trovata sulla riga della R di VERME, e cioè con la I.

Il vantaggio rispetto ai codici mono-alfabetici è evidente: la stessa lettera del testo chiaro non è sempre cifrata con la stessa lettera; e questo rende più difficile l'analisi statistica del testo cifrato e la decrittazione.

Chi riceve il messaggio per decifrarlo deve semplicemente usare il metodo inverso (sottrarre invece che sommare); riferendosi all'esempio di sopra si avrà:

Testo cifrato -	VVIUZVRFUVDRWAVUM
Chiave -	VERMEVERMEVERMEVE
Testo chiaro -	ARRIVANOIRINFORZI

si potrà decifrare la seconda V ricercandola nella riga della corrispondente lettera della chiave, la E; la colonna dove si trova la V ha al primo posto in alto la lettera chiara, la R.

SCHEDA N° 7 – CRITTOGRAFIA

Utilizzando la tabella diVigénère, inserisci un testo nelle righe seguenti e in quelle successive in testo criptato utilizzando la parola chiave “pascal”:

Testo in chiaro:

Chiave:

Testo criptato:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y