# Fondamenti di Matematica del Discreto
## Guida agli esercizi
### Prima Parte

**Algoritmo di Euclide per il calcolo del M.C.D. Tra a&b**
a=387, b=144

a/b=387/144=2 r=99
b/r=144/99=1 $r_1$=45
r/$r_1$=99/45=2 $r_2$=5
$r_1$/$r_2$=45/5=9 $r_3$=0 quindi M.C.D.(387,144)=9

**Cambio di base per numeri con la virgola**
Es: trasformare $7{,}2_{10}$ in base 6.

1) trasformo la parte intera: $7_{10}=11_6$
2) moltiplico la parte decimale per la base: 0,2*6=1,2
3) tolgo la parte intera: 1,2-1=0,2
4) moltiplico per la base: 0,2*6=1,2

è la parte decimale nella nuova base. Quindi $7{,}2_{10}=11{,}(1)_6$ Le parentesi indicano il periodo.

Es2: trasformare $347{,}6_{10}$ in base 7.

347 | 4
49 | 0
7 | 0
1 | 1 ↑
0 | quindi $347_{10}=1004_7$

per la parte decimale: 0,6*7=4,2 – 4=0,2
0,2*7=1,4 – 1=0,4
0,4*7=2,8 – 2=0,8
0,8*7=5,6 – 5=0,6 ho ottenuto il numero da cui sono partito quindi mi fermo.

$347{,}6_{10}=1004{,}(4125)_7$

**Passaggio da base b a base $b^2$**
$abcde_n=[a][bc][de]_{n^2}$ con [bc]=(b*n)+c & [de]=(d*n)+e
Es: trasformare $1004{,}(4125)_7$ in base $7^2$
[10][04],[41][25]: [10]=(1*7)+0=7, [04]=(0*7)+4=4, [41]=(4*7)+1=29, [25]=(2*7)+5=19
quindi risulta 7:4,(29;19)

**Congruenze**
$a \equiv b \bmod n$ se e solo se $a \bmod n = b \bmod n$

Proprietà:

P1)
$$ax \equiv b \bmod n \Leftrightarrow (a \bmod n)x \equiv (b \bmod n)(\bmod n)$$
$$155x \equiv 85 \bmod 6 \Leftrightarrow (155 \bmod 6)x \equiv (85 \bmod 6)(\bmod 6)$$
$$155x \equiv 85 \bmod 6 \Leftrightarrow 5x \equiv 1 \bmod 6$$


Davide Pedone, Simone Di Carlo

P2)

$$ax \equiv b \bmod n \Rightarrow kax \equiv kb \bmod n$$

$$5x \equiv 2 \bmod 7 \Rightarrow (3*5)x \equiv (2*3) \bmod 7$$

P3)

$$kax \equiv kb \bmod kn \Rightarrow ax \equiv b \bmod n$$

$$3x \equiv 3 \bmod 6 \Rightarrow x \equiv 1 \bmod 2$$

P4)

$$kax \equiv kb \bmod n \;\; se\; M.C.D.(k,n)=1 \Rightarrow ax \equiv b \bmod n$$

$$5x \equiv 5 \bmod 2 \Rightarrow x \equiv 1 \bmod 2$$

P5)

$$kax \equiv kb \bmod n \, (k \neq 0) \Rightarrow ax \equiv b \bmod (n / M.C.D.(k,n))$$

$$6x \equiv 6 \bmod 21 \Rightarrow x \equiv 1 \bmod (21/3) \Rightarrow x \equiv 1 \bmod 7$$

P6)

$$ax \equiv b \bmod n, \, d|n \Rightarrow ax \equiv b \bmod d$$

$$3x \equiv 4 \bmod 10 \Rightarrow 3x \equiv 4 \bmod 2 \;\; o \;\; 3x \equiv 4 \bmod 5$$

$$3x \equiv 4 \bmod 2 \Rightarrow (3 \bmod 2)\, x \equiv (4 \bmod 2) \bmod 2 \Rightarrow x \equiv 0 \bmod 2$$

P7)

$$ax \equiv b \bmod r \;\; e \;\; ax \equiv b \bmod s \Rightarrow ax \equiv b \bmod (m.c.m.(r,s))$$

$$5x \equiv 4 \bmod 9 \;\; e \;\; 5x \equiv 4 \bmod 6 \Rightarrow 5x \equiv 4 \bmod 18$$

Per risolvere gli esercizi occorre applicare queste proprietà.

**Congruenze del tipo** $x^y \equiv w^z$

Teorema di Fermat:

$$a^{p-1} \equiv 1 \bmod p, \; se \; p \; è \; primo$$

Teorema di Eulero-Fermat:

$$a^{\varphi(n)} \equiv 1 \bmod n, \; se \; n \; non \; è \; un \; numero \; primo$$

Es: $231^{44} \equiv 88^{72} \bmod 5$ , porto tutto in mod 5: $1^{44} \equiv 3^{72} \bmod 5 \Rightarrow 1 \equiv 3^{72} \bmod 5$

72 non è un numero primo, quindi applico Eulero.

φ(5)=4 (φ(n) è il numero di interi positivi minori o uguali a n, primi con n)

$$a^4 \equiv 1 \bmod 5 \; M.C.D.(5,1)=1 \Rightarrow 3^4 \equiv 1 \bmod 5$$

$$3^{72} = (3^4)^{18} \Rightarrow 1 \equiv 1^{18} \bmod 5 \Rightarrow 1 \equiv 1 \bmod 5, \; VERIFICATA$$

Es2: $97^{37} \equiv 11^{134} \bmod 7$

$6^{37} \equiv 4^{134} \bmod 7$ 7 è un numero primo, quindi applico Fermat

$$a^{7-1} \equiv 1 \bmod 7 \Rightarrow a^6 \equiv 1 \bmod 7$$

$$(6^6)^6 * 6 \equiv (4^6)^{22} * 4^2 \bmod 7 \Rightarrow 1^6 * 6 \equiv 1^{22} * 16 \bmod 7 \Rightarrow 6 \equiv 2 \bmod 7, \; NON\; VERIFICATA$$

**Calcolare l'inverso**

Trovare l'inverso di 4 in mod 9:

$4 \cdot a \equiv 1 \bmod 9$ a è l'inverso, ossia quel numero che moltiplicato per quattro e diviso per nove da resto 1.

**Sistemi di congruenze**

$$\begin{cases} 4x \equiv 3 \bmod 9 \\ 5x \equiv 1 \bmod 6 \end{cases} \quad calcolo \; l'inverso \; di \; 4 \; e \; 5$$

L'inverso di 4 è 7 infatti: 7*4=28 28/9= 3 Resto 1
L'inverso di 5 è 5 infatti 5*5=25 25/6=4 Resto 1
Moltiplico per l'inverso nelle due congruenze:

$$\begin{cases}(4\cdot 7)\,x\equiv 3\cdot 7\,mod\,9\\(5\cdot 5)\,x\equiv 1\cdot 5\,mod\,6\end{cases}\Rightarrow\begin{cases}28\text{x}\equiv 21\,mod\,9\\25\text{x}\equiv 5\,mod\,6\end{cases}\;trasformo\,nei\,rispettivi\,mod$$

$$\begin{cases}x\equiv 0\,mod\,3(\,per\,P6)\\x\equiv 5\,mod\,6\end{cases}\;non\,verificata$$

In generale vale la regola:

$$\begin{cases}x\equiv a\,mod\,b\\x\equiv c\,mod\,d\end{cases}\;trovo\,b\cdot h\,tale\,che:$$

$$a+b\cdot h\equiv c\,mod\,d$$

la soluzione finale del sistema è:

$$x=(a+b\cdot h)+(b\cdot d)\cdot k$$

Es2:

$$\begin{cases}5\text{x}\equiv 11\,mod\,13\\11\text{x}\equiv 4\,mod\,7\end{cases}$$

$$porto\,nei\,rispettivi\,mod:\begin{cases}5\text{x}\equiv 11\,mod\,13\Rightarrow trovo\,l'\,inverso(8)\\4\text{x}\equiv 4\,mod\,7\Rightarrow uso\,P4\end{cases}$$

$$\begin{cases}(5\cdot 8)\,x\equiv 11\cdot 8\,mod\,13\\x\equiv 1\,mod\,7\end{cases}\Rightarrow\begin{cases}x\equiv 10\,mod\,13\\x\equiv 1\,mod\,7\end{cases}\Rightarrow x=10+13\cdot h$$

$$se\,h=0\begin{cases}x=10\\10\equiv 1\,mod\,7\,?\,NO\,!\end{cases};\,se\,h=1\begin{cases}x=23\\23\equiv 1\,mod\,7\,?\,NO\,!\end{cases};\,se\,h=2\begin{cases}x=36\\36\equiv 1\,mod\,7\,?\,SI\,!\end{cases}$$

$$Quindi\,la\,soluzione\,del\,sistema\,è:\,x=(10+13\cdot 2)+(13\cdot 7)\cdot k\Rightarrow x=36+91\cdot k$$

**Divisibilità**
Ci sono due metodi per stabilire se un numero *a* è divisibile per un altro numero *b*.
Metodo 1:
Stabilire se 646727 è divisibile per 17 utilizzando il criterio 17*3=51

$$50\equiv -1\,mod\,51\quad 50=5\cdot 10,\;\;MCD(5{,}17)=1$$
$$646727\Rightarrow(64672\cdot 10)+7\Rightarrow$$
$$(64672\cdot 10\cdot 5)+7\cdot 5\Rightarrow(64672\cdot 50)+35\Rightarrow(64672\cdot(-1))+35=-64672+35=-64637$$
$$64637\Rightarrow(6463\cdot 10)+7\Rightarrow(6463\cdot 50)+35=-6428$$
$$6428\Rightarrow(642\cdot 10)+8\Rightarrow(642\cdot 50)+40=-602$$
$$602\Rightarrow(60\cdot 10)+2\Rightarrow(60\cdot 50)+10=-50,\;\;non\,congruo\,a\,0\Rightarrow 646727\,non\,divisibile\,per\,17$$

Stabilire se 615908 è divisibile per 31

$$30\equiv -1\,mod\,31$$
$$615908\Rightarrow(61590\cdot 10)+8\Rightarrow(61590\cdot 10\cdot 3)+8\cdot 3\Rightarrow(61590\cdot 30)+24=-61590+24=-61566$$
$$61566\Rightarrow(6156\cdot 10)+6\Rightarrow(6156\cdot 30)+18=-6138$$
$$6138\Rightarrow(613\cdot 10)+8\Rightarrow(613\cdot 30)+24=-589$$
$$589\Rightarrow(58\cdot 10)+9\Rightarrow(58\cdot 30)+27=-31,\;\;divisibile\,per\,31\Rightarrow 615908\,divisibile\,per\,31$$

Metodo 2:
Stabilire se 646727 è divisibile per 31

$$6\cdot 10^5+4\cdot 10^4+6\cdot 10^3+7\cdot 10^2+2\cdot 10^1+7\cdot 10^0$$

calcolo i resti delle potenze di 10 (ossia calcolo le potenze di 10 mod 31)

$10^5=100000 \Rightarrow 100000 \equiv 25\, mod\, 31,$

$10^4=10000 \Rightarrow 10000 \equiv 18\, mod\, 31,\ 10^3=1000 \Rightarrow 1000 \equiv 8\, mod\, 31,\ 10^2=100 \Rightarrow 100 \equiv 7\, mod\, 31$

$10^1=10 \Rightarrow 10 \equiv 10\, mod\, 31,\ 10^0=1 \Rightarrow 1 \equiv 1\, mod\, 31$

sostituisco nella prima formula al posto delle potenze di 10 i resti trovati

$6\cdot 25+4\cdot 18+6\cdot 8+7\cdot 7+2\cdot 10+7\cdot 1$

$6\cdot 25=150, 150 \equiv -5\, mod\, 31;\ 4\cdot 18=72, 72 \equiv 10\, mod\, 31;\ 6\cdot 8=48, 48 \equiv 17\, mod\, 31$

$7\cdot 7=49, 49 \equiv 18\, mod\, 31;\ 2\cdot 10=20, 20 \equiv 20\, mod\, 31;\ 7 \equiv 7\, mod\, 31$

$(-5)+10+17+18+20+7=67 \Rightarrow non\ divisibile\ per\ 31$

**Equazioni Diofantee**

$a\cdot x+b\cdot y=c$ ammette soluzione se e solo se $c\ multiplo\ di\ MCD(a, b)$

Esempio

$2x+3y=12$ Calcolo MCD(2,3)=1; 12 è un multiplo di 1 quindi l'equazione è risolvibile.

So che:

$ax \equiv c\, mod\, b \quad oppure \quad by \equiv c\, mod\, a \quad quindi:$

$2x \equiv 12\, mod\, 3 \quad \vee \quad 3y \equiv 12\, mod\, 2 \quad porto\ nei\ rispettivi\ mod\ e\ scelgo\ la\ più'\ comoda'$

$2x \equiv 0\, mod\, 3 \quad \vee \quad y \equiv 0\, mod\, 2 \quad scelgo\ la\ II \Rightarrow y=0+2\cdot h \Rightarrow y=2h \Rightarrow 2x+3\cdot(2h)=12$

$$2x+6h=12 \Rightarrow 2x=12-6h \Rightarrow x=6-3h \Rightarrow \begin{cases} x=6-3h \\ y=2h \end{cases}$$

Esempio 2:

Determinare il più piccolo p>2 per cui 7x+3y=p ammette soluzioni e calcolarle.

MCD(7,3)=1, il più piccolo multiplo di 1 maggiore di 2 è 3, quindi p=3

$7x \equiv 3\, mod\, 3 \quad \vee \quad 3y \equiv 3\, mod\, 7 \Rightarrow x \equiv 0\, mod\, 3 \quad \vee \quad 3y \equiv 3\, mod\, 7;\ scelgo\ la\ prima$

$$x=0+3h \Rightarrow 7\cdot(3h)+3y=3 \Rightarrow 3y=3-21h \Rightarrow \begin{cases} x=3h \\ y=1-7h \end{cases}$$

**Gruppi di sostituzioni**

$f=(1\ 5\ 2\ 4\ 3) \Rightarrow f^{-1}=(1\ 3\ 4\ 2\ 5)$

Esempio:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 3 & 6 & 4 \end{pmatrix}$ Cosa vuol dire? Descrive le trasformazioni, la prima riga elenca gli elementi, la seconda come cambiano, cioè:

1 diventa 5,
2 diventa 2,
3 diventa 1,
4 diventa 3,
5 diventa 6,
6 diventa 4. Quindi partendo da 1 vado in 5, da 5 in 6, da 6 in 4, da 4 in 3, da 3 in 1. Allora posso scriverla così: $(1\ 5\ 6\ 4\ 3)$

Ogni permutazione (o sostituzione) può essere scritta, in modo unico, come prodotto di cicli disgiunti. Come si fa?

$\alpha=(1\ 5\ 2\ 8)(3\ 7\ 2\ 4\ 5\ 8)(1\ 4\ 8\ 3\ 6)$ Si va **<u>da destra a sinistra</u>**, parto da 1 e vado a vedere in cosa di trasforma: 1 va in 4, (mi sposto nel secondo gruppo) 4 va in 5, (mi sposto nel terzo), 5 va in 2. Sono partito da 1 e sono arrivato in 2, quindi 1 va in 2. Comincio a compilare il prodotto di cicli disgiunti:

$\alpha=(1\ 2$ riparto: 2 nel primo gruppo non c'è, questo vuol dire che 2 va in 2, ossia non cambia, mi sposto nel secondo 2 va in 4, nel terzo 4 va in 4. Quindi 2 va in 4.

$\alpha=(1\ 2\ 4$ proseguo in questo modo e ottengo $\alpha=(1\ 2\ 4\ 3\ 6\ 5$
5 va in 5, mi sposto 5 va in 8, mi sposto 8 va in 1. 5 va in 1 quindi il ciclo si chiude.

$\alpha=(1\ 2\ 4\ 3\ 6\ 5)$ Gli elementi di α da cui sono partito sono 8, a={1,2,3,4,5,6,7,8}.
Nel nuovo ciclo che ho scritto ne compaiono 6, mancano {7} e {8} che quindi compongono un ciclo tra di loro. Infatti 7 va in 7, 7 va in 2, 2 va in 8.
Quindi se voglio scrivere α come prodotto di cicli disgiunti sarà: $\alpha=(1\ 2\ 4\ 3\ 6\ 5)(7\ 8)$
Vediamo un altro esempio per togliere ogni dubbio.

$\alpha=(0\ 5\ 2\ 8\ 1)(4\ 9\ 6\ 1)(2\ 8\ 3)(0\ 2\ 4\ 9\ 3)\Rightarrow\alpha=(0\ 1\ 4\ 6)(2\ 9\ 8\ 3\ 5)$ L'unico elemento che manca è 7, ma non comparendo mai significa che non cambia, quindi non lo scrivo.
**N.B:** poiché si tratta di cicli non è importante da quale elemento si parte, io vado in ordine per comodità (parto dal minor elemento non ancora utilizzato) ma:

$(0\ 1\ 4\ 6)=(1\ 4\ 6\ 0)=(4\ 6\ 0\ 1)=(6\ 0\ 1\ 4)$ *quindi scrivere* $\alpha=(0\ 1\ 4\ 6)(2\ 9\ 8\ 3\ 5)$

*o, ad esempio,* $\alpha=(6\ 0\ 1\ 4)(3\ 5\ 2\ 9\ 8)$ *è la stessa cosa!!!!*

**Parità e disparità**
Per calcolarle la parità di una sostituzione occorre scriverla come prodotto di trasposizioni e poi contare il numero di trasposizioni.

$(1\ 2\ 4\ 3\ 6\ 5)(8\ 7)\Rightarrow(1\ 2)(1\ 4)(1\ 3)(1\ 6)(1\ 5)(7\ 8)\Rightarrow 6\Rightarrow PARI$

$(0\ 1\ 4\ 6)(3\ 5\ 2\ 9\ 8)\Rightarrow(0\ 1)(0\ 4)(0\ 6)(3\ 5)(3\ 2)(3\ 9)(3\ 8)\Rightarrow 7\Rightarrow DISPARI$

**Periodo di un elemento di un gruppo finito**
Periodo di un ciclo
caso1: $p=(1\ 3\ 6\ 8\ 2\ 5\ 4)$ il ciclo ha lunghezza 7 (formato da 7 elementi), quindi il periodo di p è 7
caso2: $q=(1\ 3\ 5\ 2)(4\ 6\ 7)$ lunghezza cicli 4 e 3. m.c.m(4,3)=12, quindi il periodo di q è 12
**IMPORTANTE:**
Con u definiamo l'elemento neutro rispetto all'operazione.

$a^0=u\ \ a^1=u\circ a\ \ a^2=u\circ a\circ a$ e così via.

Ad esempio se $\circ$ corrisponde alla somma: $a^0=0\ \ a^1=0+a\ \ a^2=0+a+a=2a$

**N.B:** Sia p un elemento di periodo 12. Che periodo hanno $p^{3,}\ p^{5,}\ p^{8,}\ p^{9,}\ p^{10}$ ?
Come fare a calcolare il periodo di $q^b$ *se* $q$ *ha periodo* $a$ ?

1) Calcolo $\text{M.C.D.(a,b)}$
2) Calcolo $\text{m.c.m.}=\frac{(a\cdot b)}{\text{M.C.D.}}$
3) $\text{periodo}=\frac{\text{m.c.m.}}{b}$

Nel nostro esercizio:

$p^{12}=(p^3)^4=id\Rightarrow p^3\ ha\ periodo\ 4$

$p^5:\text{MCD}(5,12)=1,\ \text{mcm}(5,12)=60,\ 60/5=12\Rightarrow p^5\ ha\ periodo\ 12$

$p^8:\text{MCD}(8,12)=4,\ \text{mcm}(8,12)=24,\ 24/8=3\Rightarrow p^8\ ha\ periodo\ 3$

$p^9:\text{MCD}(9,12)=3,\ \text{mcm}(9,12)=36,\ 36/9=4\Rightarrow p^9\ ha\ periodo\ 4$

$p^{10}:\text{MCD}(10,12)=2,\ \text{mcm}(10,12)=60,\ 60/10=6\Rightarrow p^{10}\ ha\ periodo\ 6$

**Sottogruppi**
$S_6$={1,2,3,4,5,6} $\alpha=(2\ 6\ 3\ 5)(4\ 6\ 5)(3\ 4\ 6)(1\ 5\ 3)\Rightarrow\alpha=(1\ 4\ 2\ 6\ 5\ 3)$ H è un sottogruppo di $S_6$ generato da α. Calcolare ordine e elementi di H.

L'ordine del sottogruppo coincide con il periodo del generatore. α ha periodo 6 quindi gli elementi di H sono $\mathrm{H}=\{\alpha, \alpha^{2,} \alpha^{3,} \alpha^{4,} \alpha^{5,} \alpha^{6}=id\}$

$\alpha^2=(142653)(142653)=(125)(346)$; $\alpha^3=(124653)(125)(346)=(16)(23)(45)$

$\alpha^4=(142653)(16)(23)(45)=(152)(364)$; $\alpha^5=(124653)(152)(364)=(135624)$

Per calcolare il laterale destro di α dato da, per esempio, (123) faccio semplicemente α(123); per il sinistro (123)α.

Sottogruppi di $(\mathbb{Z}_{12}^*, x)=\{1,5,7,11\}$
il periodo di 1=1 per convenzione
il periodo di 5: $5^n\equiv 1\, mod\ 12$ , se n=2 $5^2\equiv 1\, mod\ 12 \Rightarrow$ il periodo di 5 in $\mathbb{Z}_{12}^*$ è 2 , sottogr. {1,5}
il periodo di 7: $7^2\equiv 1\, mod\ 12 \Rightarrow$ il periodo di 7 è 2 , sottogruppo {1,7}
il periodio di 11: $11^2\equiv 1\, mod\ 12 \Rightarrow$ il periodo di 11 è 2 , sottogruppo {1,11}
L'ordine del sottogruppo deve essere un divisore dell'ordine del gruppo.

Sottogruppi di $(\mathbb{Z}_{16}^*, x)=\{1,3,5,7,9,11,13,15\}$
L'ordine di $\mathbb{Z}_{16}^*$ è 8 quindi l'ordine dei sottogruppi può essere 2 o 4.

**Gruppi ciclici**
Trovare un generatore diverso da 1 per: $\mathbb{Z}_8, + =\{0,1,2,3,4,5,6,7\}$
Un generatore è un elemento appartenente al gruppo su cui continuando ad eseguire l'operazione del gruppo ottengo tutti gli elementi.
Nell'esercizio:

$1: 1^0=0,\ 1^1=1,\ 1^2=1+1=2,\ 1^3=1+1+1=3...1^7=7$ ok, è un generatore

$2: 2^0=0,\ 2^1=2,\ 2^2=4,\ 2^3=6,\ 2^4=8(\text{in}\, mod8=0),\ 2^5=10=2\Rightarrow\{0,2,4,6\}$ 2 non è un generatore

$3: 3^0=0,\ 3^1=3,\ 3^2=6,\ 3^3=9=1,\ 3^4=12=4,\ 3^5=15=7,\ 3^6=18=2,\ 3^7=21=5$

$\Rightarrow\{0,1,2,3,4,5,6,7\}\Rightarrow 3$ è un generatore

**Omomorfismi**
Per svolgere gli esercizi bisogna prima osservare se il primo gruppo (dominio) è ciclico.
***Se è ciclico*** l'esercizio è facile, devo solo costruire la *tavola pitagorica* degli omomorfismi.
Si fa così:

1. nella prima colonna un generatore e le sue potenze (ad esempio h)
2. nella prima riga gli elementi del codomio
3. nella seconda riga copio gli elementi della prima riga
4. si riempiono le colonne applicando le potenze del generatore all'elemento del codominio. (tenere conto dell'operazione e del numero di elementi del codominio; se sono in $(\mathbb{Z}_7, +)$ $2^3=2+2+2=8$, che in $mod7$ fa 1 )

Esempio:

$G\rightarrow(\mathbb{Z}_7^*, \mathrm{x})$

G è ciclico per ipotesi, elemento generatore "q", ordine 4
$(\mathbb{Z}_7^*, \mathrm{x})$ è ciclico, i suoi elementi sono {1,2,3,4,5,6}

| *f* | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| **q** | 1 | 2 | 3 | 4 | 5 | 6 |
| **$q^2$** | $1^2$=1 | 22=4 | 2 | 2 | 4 | 1 |
| **$q^3$** | 1 | 23=8mod7=1 | 6 | 1 | 6 | 6 |
| **$q^4$=id** | 1 | 2 | 4 | 4 | 2 | 1 |
| **Ker {f}** | X | NO | NO | NO | NO | {$q^2$,id} |
| **Img {f}** | {1} | NO | NO | NO | NO | {1,6} |

Se c'è omomorfismo il nucleo è composto dalle potenze del generatore che danno il neutro dell'operazione (in questo caso 1).

***Se non è ciclico*** si utilizzano gli ordini di nucleo e immagini.
Il teorema dell'ordine dice che l'ordine del dominio è dato dal prodotto di ordine del nucleo e ordine dell'immagine.

*Ord(dominio)= Ord(ker) x Ord(img)*

Un nucleo è l'insieme degli elementi che vengono trasformati nel neutro del codominio.
L'immagine è l'insieme degli elementi che sono trasformati negli elementi del dominio.
Esempio:

$(\mathbb{Z}_{12}^*, \mathrm{x}) \rightarrow (\mathbb{Z}_{14}^*, \mathrm{x})$

$(\mathbb{Z}_{12}^*, \mathrm{x})$ ha elementi {1,5,7,11}, quindi ordine 4 e non è ciclico

$(\mathbb{Z}_{14}^*, \mathrm{x})$ ha elementi {1,3,5,9,11,13}, quindi ordine 6 ed è ciclico

Ord(dominio)=4 quindi 4=Ord(ker) x Ord(img)
4=1x4 non è omomorfismo perchè non esistono immagini di ordine 4
4=4x1 è l'omomorfismo banale
4=2x2 devo trovare l'immagine, ossia un sottogruppo di dimensione 2 di $\mathbb{Z}_{14}$

**n-1 ha sempre periodo 2 in** $\mathbb{Z}_n$ , quindi come immagine prendo {1,13}

ora costruisco la tabella:
Guardo gli elementi del nucleo e metto 1 in corrispondenza di quei valori nelle colonne, 13 nelle altre. Otterrò la seguente tabella:

| **Nucleo** | **Immagine** | **1** | **5** | **7** | **11** |
|---|---|---|---|---|---|
| 1,5 | 1,13 | 1 | 1 | 13 | 13 |
| 1,7 | 1,13 | 1 | 13 | 1 | 13 |
| 1,11 | 1,13 | 1 | 13 | 13 | 1 |
| 1,5,7,11 | 1,13 | 1 | 1 | 1 | 1 |

# Seconda Parte

**Autovalori, autovettori e diagonalizzazione**

Prendiamo ad esempio la matrice di ordine n=3, $\begin{bmatrix} 7 & 0 & 0 \\ 1 & 9 & 0 \\ -1 & 16 & 7 \end{bmatrix}$ devo calcolare le soluzioni del polinomio caratteristico che è dato da det(A-hI)=0.

A è la matrice data, I è la matrice identità $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

il polinomio caratteristico sarà quindi così: $\begin{bmatrix} (7-h) & 0 & 0 \\ 1 & (9-h) & 0 \\ -1 & 16 & (7-h) \end{bmatrix}$ e il suo determinante sarà dato da $(7-h)^2(9-h)=0$

Ho trovato gli autovalori 7 e 9, ossia le soluzioni dell'equazione.
La molteplicità algebrica $m_a$ di 9 è 1, poiché l'esponente di (9-h) è appunto 1.
La molteplicità algebrica $m_a$ di 7 è 2.
Ci sono due possibilità per capire se una matrice è diagonalizzabile.

1. La somma delle molteplicità algebriche degli autovalori di A è uguale all'ordine di A
2. Gli autovalori di A sono tutti regolari, ossia $m_a(h)=m_g(h)$

È sufficiente una di queste due condizioni affinchè la matrice sia diagonalizzabile.
**N.B.** Se gli autovalori sono distinti la matrice è sempre diagonalizzabile!
La molteplicità geometrica di A è pari alla dimensione dell'autospazio relativo all'autovalore A, in particolare $m_g$=n-rK(A-AI)

$$m_a(9)=1 \quad m_g(9)=3-rk\begin{bmatrix} (7-9) & 0 & 0 \\ 1 & (9-9) & 0 \\ -1 & 16 & (7-9) \end{bmatrix} \quad rk\begin{bmatrix} -2 & 0 & 0 \\ 1 & 0 & 0 \\ -1 & 16 & -2 \end{bmatrix}=2 \quad m_g(9)=3-2=1$$

$$m_a(7)=2 \quad m_g(7)=3-rk\begin{bmatrix} (7-7) & 0 & 0 \\ 1 & (9-7) & 0 \\ -1 & 16 & (7-7) \end{bmatrix} \quad rk\begin{bmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \\ -1 & 16 & 0 \end{bmatrix}=2 \quad m_g(7)=3-2=1$$

**N.B:** Controllare che se $m_a(h_1)+m_a(h_2)+...+m_a(hn)=n$ è diagonalizzabile, in caso contrario devo confrontare $m_a$ e $m_g$ dei rispettivi autovalori.

Per calcolare gli autovettori:
imposto il sistema Av=hv, dove v è un vettore di 3 componenti (x,y,z)

$A=\begin{bmatrix} 7 & 0 & 0 \\ 1 & 9 & 0 \\ -1 & 16 & 7 \end{bmatrix} \quad v=\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ , l'autovettore relativo ad h=9 è dato da A(x,y,z)=9(x,y,z) che da luogo al sistema: $\begin{cases} 7\mathrm{x}=9\mathrm{x} \\ x+9\mathrm{y}=9\mathrm{y} \\ -x+16\mathrm{y}+7\mathrm{z}=9\mathrm{z} \end{cases} \Rightarrow \begin{cases} x=0 \\ y=y \\ z=8\mathrm{y} \end{cases} \Rightarrow$ l'autovettore relativo all'autovalore 9 è $\begin{bmatrix} 0 \\ y \\ 8\mathrm{y} \end{bmatrix}$

Per l'autovalore 7:

$$\begin{cases} 7\mathrm{x}=7\mathrm{x} \\ x+9\mathrm{y}=7\mathrm{y} \\ -x+16\mathrm{y}+7\mathrm{z}=7\mathrm{z} \end{cases} \Rightarrow \begin{cases} x=x \\ y=-x/2 \\ x=0 \end{cases} \Rightarrow \text{l'autovettore relativo a 7 è} \begin{bmatrix} 0 \\ 0 \\ z \end{bmatrix}$$

**Sistemi di generatori, basi e componenti di un vettore**

Stabilire se $v_1$ e $v_2$ sono generatori di $v_3$.

**Unione, intersezione e somma di sottospazi**

La dimensione di una base è data dal numero di vettori da cui è composta.
**N.B:** Sia V uno spazio vettoriale di dimensione n su K e siano S e T due suoi sottospazi.
dim(S+T)=dim(S)+dim(T)-dim(S∩T)

Es: in $R^3$ si considerino i due sottospazi S e T definiti nel modo seguente.

$$S=\left\{\begin{bmatrix} a \\ b \\ c \end{bmatrix}\in \mathbb{R}^3 : a+2b-c=0\right\},\quad T=\left\{\begin{bmatrix} a \\ b \\ c \end{bmatrix}=h\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}+k\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}\right\}$$

Dopo aver determinato una base per S e T, determinare la dimensione e una base per S∩T e S+T.

Si può esprimere il generico vettore di S come $S=\left\{\begin{bmatrix} a \\ b \\ a+2b \end{bmatrix}\right\}, \Rightarrow \text{una base è } S=\left\{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix},\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}\right\}$

quindi la dimensione di S è 2. (per trovare i due vettori della base di S occorre semplicemente assegnare dei valori “comodi” ad a e b)

Per quanto riguarda T una base sono i due vettori che lo generano $\left\{\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix},\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}\right\}$ , quindi anche in questo caso la dimensione è 2.

Quindi, dato che S+T è contenuto in $R^3$, la dimensione massima sarà 3:

| **dim(S+T)=** | **dim(S)+** | **dim(T)** | **-dim(S∩T)** |
|---|---|---|---|
| 3= | 2+ | 2 | -1 |
| 2= | 2+ | 2 | -1 |

Calcolo S∩T. Il generico vettore di T $\begin{bmatrix} (h+2k) \\ k \\ -h \end{bmatrix}$ sta in S se le sue componenti soddisfano la relazione che definisce i vettori di S:

$$(h+2k)+2k+h=0 \Rightarrow 2h+4k=0 \Rightarrow h=-2k \begin{bmatrix} 0 \\ k \\ 2k \end{bmatrix}=k\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

quindi la dimensione di (S∩T)=1, quindi S+T=$R^3$, quindi una sua base è la canonica di $R^3$.

Es2: Si consideri il sottospazio di R3 $X=\left\{\begin{bmatrix} a \\ b \\ c \end{bmatrix}: a+2c=0\right\}$

a) determinare la dimensione e una base per X
b) determinare due diversi sottospazi complementari di X in $R^3$

DimX=2, infatti una base è $\begin{bmatrix} -2c \\ b \\ c \end{bmatrix} = b \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + c \begin{bmatrix} -2 \\ 0 \\ 1 \end{bmatrix}$

Gli spazi generati rispettivamente da un vettore qualsiasi che completi la base di X, ad esempio da i oppure da k, sono spazi complementari.

**Omomorfismi, nucleo e immagine**

Teorema importante: **Teorema di nullità più rango** Se dimV=*n*, dimV = dim Ker*f* +dim *f(v)*

Es: Si dimostri che esiste uno ed un solo omomorfismo $f : R^3 \to R^3$ tale che:

$$f \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 0 \end{bmatrix}, f \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \\ 4 \end{bmatrix}, f \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ -4 \end{bmatrix}$$

Il teorema di determinazione di un omomorfismo garantisce la proprietà se i tre vettori

$\begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix}$ sono una base, e infatti: $det \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 0 & 1 & 0 \end{bmatrix} = -2 \neq 0$

I vettori sono una base perchè il determinante è diverso da zero, quindi l'omomorfismo c'è ed è unico.

- Per sapere se è un immagine devo prendere i vettori e farne la combinazione lineare. ($a*v_1+b*v_2+c*v_3+...$=Immagine)
- Per trovare la base dell'immagine, faccio la canonica dei vettori, tengo solo quelli indipendenti (det≠0) e l'immagine è tutto il codominio.
- Se ho due vettori base e un immagine "presunta" come prima faccio a*v1+b*v2=Immagine; se a e b esistono allora esiste anche l'immagine, altrimenti vuol dire che l'immagine "presunta" non appartiene al codominio (non è immagine)

**Omomorfismi e matrici**

Dati i vettori faccio la canonica di ogni vettore e trovo la matrice associata.

Es: Si consideri l'omomorfismo $f : R^3 \to R^3 \; definito \; da \; f \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 2a+3b \\ b-a+2c \\ a+4b+2c \end{bmatrix}$ ; determinare la matrice **A** associata ad *f* rispetto alla base canonica di $R^3$

Risulta:

$f \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ -1 \\ -1 \end{bmatrix}, f \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}, f \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}$ ma è $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + z \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \Rightarrow A = \begin{bmatrix} 2 & 3 & 0 \\ -1 & 1 & 2 \\ 1 & 4 & 2 \end{bmatrix}$

Per trovare il nucleo devo mettere le equazioni uguali a zero. (attenzione a non eliminare le incognite!)

$$f \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 2a+3b \\ b-a+2c \\ a+4b+2c \end{bmatrix} = 0 \Rightarrow \begin{cases} a+2b=0 \\ b-a+2c=0 \\ a+4b+2c=0 \end{cases} \Rightarrow \begin{cases} a=-2b \\ -4b+b+3b=0 \\ c=3b \end{cases} \Rightarrow \begin{cases} a=-2b \\ c=3b \end{cases}$$