

CORSO DI
MATEMATICA DISCRETA

Prof. Fabio DI FRANCO

**Programma del Corso di: MATEMATICA DISCRETA
(A.A. 2000/2001)**

Elementi di logica. Nozioni base di insiemistica. Assioma del buon ordinamento e principio di induzione.

Aritmetica: algoritmo della divisione, scrittura di un intero in base >1 , divisori e multipli, massimo comune divisore, algoritmo di Euclide delle divisioni successive. Numeri primi e fattorizzazione unica, applicazione alla non finitezza dell'insieme dei numeri primi ed all'irrazionalità di alcuni numeri reali.

Relazioni fra insiemi. Relazioni di equivalenza e classi di equivalenza. Relazione di congruenza e classi di congruenza. Applicazioni fra insiemi: applicazioni iniettive, surgettive, biunivoche. Applicazione inversa di una applicazione biunivoca. Composizione di applicazioni. Principio dei "cassetti". Numero delle applicazioni fra insiemi finiti. Numero delle applicazioni iniettive tra insiemi.

Disposizioni e combinazioni. Coefficiente binomiale e sue proprietà. Triangolo di Tartaglia. Prodotto cartesiano. Matrici e prodotto di matrici. Prodotto booleano di matrici. Sviluppo della potenza del binomio di Newton. Metodo del "contare per righe e colonne".

Permutazioni: decomposizione in cicli, trasposizioni, inversioni, parità di una permutazione. Determinante di una matrice quadrata, regola di Laplace. Teorema di Cramer. Rango di una matrice. Teorema di Rouché-Capelli. Risolubilità dei sistemi lineari.

Principio delle somma. Principio di inclusione-esclusione: il problema della "segretaria distratta"; la funzione di Eulero. Partizioni di un insieme finito, numeri di Stirling, numero delle applicazioni surgettive fra insiemi finiti.

Disegni. 2-disegni e piani proiettivi. Cammini Euleriani ed Hamiltoniani. Colorazione e numero cromatico. Matrice di adiacenza di un grafo.

Operazioni in un insieme: monoidi, gruppi. Gruppo delle applicazioni biunivoche da un insieme in se stesso. Elementi simmetrizzabili in un monoide. Operazioni fra le classi di congruenza.

Elementi di teoria dei gruppi. Elementi simmetrizzabili in Z_n . Potenze di un elemento di un gruppo, periodo di un elemento, teorema di Lagrange. Applicazione aritmetica: teorema di Eulero-Fermat.

Crittografia.

Lezione n°. 1 - 16 ott. 2000

Presentazione del corso. Corso annuale di circa 60h. Le lezioni dureranno fino a maggio circa, con le interruzioni di 3 settimane circa a Natale e di 2 settimane circa a Pasqua.

Bisogna assistere ad almeno il 75% delle lezioni.

Gli appelli sono 7 all'anno, così suddivisi: 1 a giugno, 1 a luglio, 1 a settembre, 1 ad ottobre, 1 a dicembre, 1 a febbraio ed 1 ad aprile.

L'esame si svolge con una prova scritta (che non è selettiva ma contribuisce alla votazione finale) ed una prova orale.

Testo consigliato: N.L. Biggs, "Discrete mathematics", Ed. Clarendon Press – Oxford.

Il libro di testo suggerito non è indispensabile perché possono bastare gli appunti presi durante le lezioni. Il prof. assegnerà anche degli esercizi da svolgere dei quali alcuni saranno corretti a lezione. Per gli altri si può comunque chiedere la correzione.

Si faranno anche alcune esercitazioni (al di fuori delle ore di lezione).

Orario di ricevimento: giovedì e venerdì dalle 9,00 alle 11,00.

Introduzione.

Il corso si occupa delle "strutture discrete". Il termine *discreto* viene introdotto in contrapposizione al termine *continuo*.

Una struttura continua è una struttura nella quale fra due elementi di essa è sempre possibile inserirne un altro (continuando all'infinito). Un esempio può essere una retta su un piano nella quale tra due punti qualsiasi è sempre possibile trovarne un altro.

Nelle strutture discrete ciò non è sempre possibile, ci sono cioè delle coppie di elementi tra i quali non è possibile inserirne un terzo. Un esempio è una retta rappresentante gli interi, in cui ad esempio tra 1 e 3 si può trovare il 2 ma tra 2 e 3 non c'è un altro elemento dell'insieme.

Se ne deduce che una struttura continua contiene infiniti elementi. (Notare che non sempre è vero il viceversa, cioè l'avere infiniti elementi non implica l'essere continuo).

Ciò non significa che una struttura discreta non possa contenere infiniti elementi (vedi l'esempio degli interi).

Si può invece affermare che un insieme con un numero finito di elementi è sicuramente una struttura discreta.

Lezione n°. 2 – 18 ott. 2000

Elementi di logica matematica.

La logica matematica è alla base di ogni argomento di matematica e, in definitiva, di molta parte dell'informatica.

Si studieranno le proposizioni logiche.

Si definisce *proposizione logica* una frase di senso compiuto che può essere o *vera* o *falsa*.

Schematicamente si indica con una lettera (la proposizione) seguita dal simbolo "=", e dal testo della proposizione (in genere tra " ").

Esempio:

$P = \text{"7 è un intero positivo"}$ (P è una proposizione vera)

$Q = \text{"4 è un intero dispari"}$ (Q è una proposizione falsa)

Nell'enunciare una proposizione si prescinde dalla capacità di stabilirne la veridicità.

Esempio:

$R = \text{"Esiste vita intelligente su altri pianeti"}$ è una proposizione logica, anche se non possiamo dire se sia vera o falsa.

Si definisce *predicato logico* una frase di senso compiuto che contiene delle variabili e che, a priori, non è né vera né falsa ma che diventa una proposizione logica vera o falsa non appena si attribuiscono dei valori concreti alle variabili.

Schematicamente si indica con una lettera (il predicato) seguito, tra parentesi, dall'elenco delle variabili coinvolte, seguita quindi dal simbolo "=", e dal testo del predicato (in genere tra " ").

Esempio:

$P(x,y) = \text{"x e y sono interi positivi tali che } x+y>7\text{"}$

Attribuendo dei valori alle variabili avremo delle proposizioni logiche vere o false:

$P(5,6) = \text{"5 e 6 sono interi positivi tali che } 5+6>7\text{"}$ è una proposizione logica vera,

$P(2,3) = \text{"2 e 3 sono interi positivi tali che } 2+3>7\text{"}$ è una proposizione logica falsa.

Per motivi di praticità si può indicare anche un *campo di variabilità* delle variabili, definire cioè l'insieme dei valori che le variabili possono assumere.

Esempio:

$P(x) = "x \geq 5"$ campo di variabilità = numeri razionali positivi.

$P(1/2)$ = proposizione logica falsa

$P(17/3)$ = proposizione logica vera.

Calcolo proposizionale

Definiamo le principali operazioni che si applicano sui predicati per ottenerne degli altri.

Congiunzione logica

Opera su due predicati per ottenerne un terzo.

Dati due predicati P e Q, la loro congiunzione logica è un nuovo predicato che coinvolge sia le variabili di P che le variabili di Q e che sarà VERO solo per quei valori di variabili che rendono veri sia P che Q.

La congiunzione logica si indica con $P \wedge Q$ (P and Q).

Per ottenere il testo di $P \wedge Q$ basta unire i due testi di P e Q con la congiunzione "e".

Esempio:

$P(x) = "x > 7"$ e $Q(y) = "y \text{ è pari}"$ c.v. = interi positivi

$P \wedge Q(x,y) = "x > 7 \text{ e } y \text{ è pari}"$

$P \wedge Q(9,8)$ = proposizione logica vera (sia $P(9)$ che $Q(8)$ sono proposizioni vere.

$P \wedge Q(9,5)$ = proposizione logica falsa ($P(9)$ è vera ma $Q(5)$ è falsa)

Per schematizzare si usa la tabella di verità, che va letta come una tavola pitagorica, dove si assume che 0=falso ed 1= vero.

		Valori di Q	
		0	1
Valori di P	0	0	0
	1	0	1

Disgiunzione logica

Opera su due predicati per ottenerne un terzo.

Dati due predicati P e Q, la loro disgiunzione logica è un nuovo predicato che coinvolge sia le variabili di P che le variabili di Q e che sarà VERO per quei valori di variabili che rendono vero almeno uno dei predicati di partenza.

La disgiunzione logica si indica con $P \vee Q$ (P or Q).

Per ottenere il testo di $P \vee Q$ basta unire i due testi di P e Q con la congiunzione "o" (oppure), facendo attenzione al fatto che la congiunzione "o" non ha valore esclusivo.

Notare che $P \vee Q$ è falsa solo quando sia P che Q sono falsi.

La tabella di verità è:

		Valori di Q	
		0	1
Valori di P	0	0	1
	1	1	1

Negazione logica

Opera su un solo operando.

dato un predicato P , la sua negazione logica è un altro predicato, indicato con \bar{P} (not P) che ha i valori di verità invertiti rispetto a quelli di P .

Valori di P	0	1	\bar{P} è vero solo per quei valori che rendono falso P
	1	0	\bar{P} è falso solo per quei valori che rendono vero P

Il testo di \bar{P} si può ottenere antepoendo al testo di P le parole "Non è vero che", ma questa è una formula non molto *elegante*.

Esempio:

$$P(x) = "x > 5" \quad \bar{P}(x) = "Non \text{ è vero che } x > 5"$$

Una maniera più elegante è quella di costruire una frase "positiva" cambiando il testo di P con uno che lo neghi.

Esempio:

$$P(x) = "x > 5" \quad \bar{P}(x) = "X \leq 5"$$

In questo caso bisogna però stare bene attenti nel cambiare la frase:

Esempio:

$$P(x) = "tutti \text{ gli animali dell'insieme } x \text{ sono erbivori}" \quad \text{c.v.} = \text{tutte le specie animali}$$

$$\bar{P}(x) = "esiste \text{ almeno un animale dell'insieme } x \text{ che non è erbivoro}"$$

e non "Nessun animale dell'insieme x è erbivoro".

Lezione n°. 3 – 20 ott. 2000

Dalle tre operazioni introdotte, applicate congiuntamente, se ne possono definire altre.

Esempio:

Dati i predicati P e Q, applicando la congiunzione e la negazione logica si può ottenere:

$P \wedge \bar{Q}$ (andnot) che ha la seguente tavola di verità:

		Valori di Q	
		0	1
Valori di P	0	0	0
	1	1	0

Esercizio:

Trovare la tavola di verità della seguente espressione: $(P \vee Q) \wedge \text{not}(P \wedge Q)$, che da origine all'operatore disgiunzione logica esclusiva (OR ESCLUSIVO), e verificare che essa sarà vera quando solo uno dei due predicati è vero (e quindi l'altro è falso).

		Valori di Q	
		0	1
Valori di P	0	0	1
	1	1	0

Infatti, si verifica che l'eguaglianza data sarà verificata solo per $P=0$ e $Q=1$ oppure per $P=1$ e $Q=0$, risultando invece falsa quando i due predicati hanno lo stesso valore.

Implicazione logica

Dati due predicati P e Q, coinvolgenti le stesse variabili, si dice che “P *implica* Q” (“P *segue* Q” o, ancora, “se P *segue* Q”) se, per tutti i valori delle variabili che rendono vero P, si ha che gli stessi valori rendono vero anche Q.

La notazione grafica dell'implicazione logica è il simbolo “ \Rightarrow ”. (P implica Q sarà $P \Rightarrow Q$)

Esempio:

$P(x) = “x > 8”$ e $Q(x) = “x > 5”$ c.v.: interi positivi

Si evince subito che tutti i valori che rendono vero P renderanno vero anche Q, per cui si può dire che P implica Q.

La notazione grafica per dire che P non implica Q sarà invece: $P \nRightarrow Q$.

Dire che P non implica Q significa che esiste almeno un valore delle variabili che rende vero P ma rende falso Q .

Per verificare se un predicato P implica un altro predicato Q si usano diverse tecniche.

- Per dimostrare che $P \Rightarrow Q$: preso un qualunque valore delle variabili che rende vero P , questo *deve* rendere vero anche Q (si opera in maniera generale; per indicare un *qualunque* valore si può utilizzare un letterale).
- Per dimostrare che $P \nRightarrow Q$: bisogna trovare un valore delle variabili che renda vero P ma renda falso Q (in questo caso si va alla ricerca del caso particolare).

Esempio:

Dati i predicati $P(x) = "x > 8"$ e $Q(x) = "x > 5"$ (c.v.: interi positivi)

si vuol verificare che $Q \nRightarrow P$.

Basta verificare che per uno qualsiasi dei valori di x scelto nella triade (6,7,8) Q è vero ma P è falso.

L'implicazione logica costituisce la struttura dei teoremi matematici. Se si dice che $P \Rightarrow Q$, il predicato P sarà l'*ipotesi* mentre il predicato Q costituisce la *tesi*.

Esempio:

"La somma degli angoli interni di un triangolo forma un angolo piatto" corrisponde all'implicazione $P \Rightarrow Q$, dove $P = "x \text{ è un triangolo}"$ e $Q = "la somma degli angoli interni di x è un angolo piatto"$ (c.v.: poligoni nel piano).

La dimostrazione di un teorema (e quindi di una implicazione) consiste in una serie di *passaggi logici*, che a loro volta sono delle implicazioni giustificate dall'evidenza o da conoscenze acquisite in precedenza.

Esempio:

Dati i due predicati $P = "x \text{ è un intero relativo}"$ e $Q = "x \cdot 0 = 0"$, verifichiamo che $P \Rightarrow Q$.

Partiamo dal fatto che x è un intero relativo per cui valgono le proprietà dei numeri relativi. Sappiamo che 0 è l'elemento neutro rispetto alla somma, per cui possiamo scrivere $x \cdot (0 + 0) = x \cdot 0$ che, per la proprietà distributiva diviene $x \cdot 0 + x \cdot 0 = x \cdot 0$; sappiamo che, sommando le stesse quantità ai due membri dell'uguaglianza questa non cambia:

$x*0+x*0+(-x*0) = x*0+(-x*0)$. Un intero sommato al suo opposto dà come risultato zero per cui avremo $x*0+0 = 0$ e, ricordando ancora che lo zero è neutro rispetto alla somma, otteniamo $x*0 = 0$ che è la tesi.

Esercizio:

Dimostrare la “regola dei segni”, cioè che $P \Rightarrow Q$ essendo:

$P = \text{“}x \text{ e } y \text{ sono interi relativi”}$

$Q = \text{“}x*(-y) = -(x*y)\text{”}$

Mia dimostrazione (da verificare): sappiamo che 1 è l'elemento neutro rispetto al prodotto per cui possiamo scrivere che

$x*(-y) = x*(1*(-y))$, per la proprietà commutativa del prodotto avremo che $x*(1*(-y)) = x*(-y*1) = x*(-1*y)$ quindi, applicando la proprietà distributiva del prodotto otterremo:

$x*(-1*y) = (-1*x)*y = -1*(x*y)$ essendo 1 neutro rispetto al prodotto : $-1*(x*y) = -(x*y)$ che è la tesi che volevamo dimostrare.

Altra dimostrazione: $x*0=0$ (è già dimostrato) $\Rightarrow x*[y+(-y)]=0$ (un numero sommato al suo opposto dà zero), applicando la proprietà distributiva abbiamo $x*y+x*(-y)=0$, se sommiamo ad ambo i membri la stessa quantità $(-x*y)$ otteniamo $(-x*y+x*y)+ x*(-y) = -x*y$. Da questa, visto che sommando un numero con il suo opposto si ottiene zero e che zero è l'elemento neutro rispetto alla somma, possiamo scrivere che $x*(-y) = -x*y$, che è la tesi.

Lezione n°. 4 – 23 ott. 2000

Se due predicati si implicano a vicenda ($P \Rightarrow Q$ e $Q \Rightarrow P$) si dicono **equivalenti** e ciò viene indicato con la simbologia $P \Leftrightarrow Q$ (si può anche dire “P se e solo se Q”).

Si è già detto che la struttura tipica di un teorema matematico è una implicazione dove il primo predicato è l'ipotesi ed il secondo la tesi ($P \Rightarrow Q$, P è l'ipotesi e Q la tesi).

Oltre alla *dimostrazione diretta*, che consiste nel fissare un *qualunque* valore delle variabili che rende vero P e dimostrare che rende vero anche Q, esiste anche una *dimostrazione inversa*, detta anche *dimostrazione per assurdo*: si suppone (per assurdo) che $P \nRightarrow Q$ (quindi che esiste almeno un valore delle variabili tale che P sia vero ma Q falso) e si cerca di arrivare ad una contraddizione logica. In genere si arriva ad una affermazione che è contemporaneamente vera e falsa.

Esempio:

dimostrare che se x è un intero positivo, il numero razionale $x*(x+1)/2$ è un intero.

Possiamo schematizzare: $P = "x \text{ è un intero positivo}"$, $Q = "x*(x+1)/2 \text{ è un intero}"$, dobbiamo dimostrare che $P \Rightarrow Q$.

Procedendo per assurdo ipotizziamo l'esistenza di un valore che renda vero P e falso Q , quindi che esista un intero positivo a tale che $x*(x+1)/2$ non sia un numero intero.

Allora, se $a*(a+1)/2$ non è un intero, applicando il *concetto di divisibilità e di frazione* ne seguirà che $a*(a+1)$ non è divisibile per 2, per cui $a*(a+1)$ è un numero dispari (*concetto di pari e dispari*) a quindi sia a che $(a+1)$ sono dispari (*regole sul prodotto di interi pari e dispari*) per cui ne segue che $(a+1)-a=1$ è pari (*regole sulla somma e differenza di numeri dispari*) e qui abbiamo la contraddizione logica in quanto non è vero che 1 è pari.

Regola : Quando per un'implicazione $P \Rightarrow Q$ esiste una dimostrazione diretta ne esiste anche una per assurdo e viceversa.

A volte la dimostrazione diretta è più semplice e viceversa.

Esercizio: dimostrare l'implicazione precedente per via diretta.

Esistono implicazioni $P \Rightarrow Q$ che non sono state ancora dimostrate né vere né false.

Esempi:

1) Congettura di Goldback: ogni numero intero pari più grande di 2 si può ottenere come somma di due numeri primi (anche non distinti).

Si tratta dell'implicazione $P \Rightarrow Q$ dove $P = "x \text{ è un intero pari maggiore di 2}"$ e $Q = "x \text{ è la somma di due numeri primi}"$.

Per $x=4$ possiamo scrivere $x=2+2$, per $x=6$ possiamo scrivere $x=3+3$, per $x=8$ possiamo scrivere $x=3+5$, per $x=10$ possiamo scrivere $x=5+5$ ma nessuno può dire se ciò è vero continuando all'infinito, non possiamo dimostrare cioè né che $P \Rightarrow Q$ né che $P \nRightarrow Q$.

2) Un numero intero maggiore di 1 è detto *perfetto* se coincide con la somma dei suoi divisori diversi da se stesso (es.: $6=1+2+3$ è un numero perfetto, $8 \neq 1+2+4$ non è un numero perfetto). È vero che ogni numero perfetto è pari? Non è certo.

Teoria degli insiemi (insiemistica)

Ci sono due maniere di introdurre l'insiemistica:

1. modo *assiomatico*, più preciso formalmente ma meno intuitivo;
2. *teoria ingenua degli insiemi*, meno precisa formalmente ma più intuitiva.

In questo corso ci si baserà sulla teoria ingenua degli insiemi, che si basa sul *concetto di insieme*, che non viene definito ma considerato immediatamente evidente.

Un insieme contiene elementi di natura arbitraria: se A è un insieme, per indicare che un elemento x appartiene ad A si scrive, simbolicamente, che $x \in A$; se invece x non è un elemento di A si scrive $x \notin A$.

Ci sono due modi di descrivere un insieme:

1. modo *esplicito*: si elencano gli elementi dell'insieme (es.: $A = \{a, b, c, \dots\}$);
2. modo *implicito*: si usa il concetto di predicato logico (es.: $A = \{x \text{ tale che } P(x)\}$; con questa notazione si intende cioè che l'insieme A è formato da tutti i valori di x che rendono vero il predicato $P(x)$).

La dicitura “tale che” si indica anche con il simbolo “/”. (es.: $A = \{x / x \text{ è un intero positivo}\}$).

Altri simboli che si usano in insiemistica sono:

- il simbolo \forall , che sostituisce la locuzione “per ogni” (“qualunque”, “per tutti i valori”);
- il simbolo \exists , che sostituisce la locuzione “esiste”;
- il simbolo $\exists!$, che sostituisce la locuzione “esiste un solo” (“esiste ed è unico”).

Se $P(x)$ è un predicato che è falso per ogni valore della variabile x , l'insieme dei valori denotato non contiene elementi ed è definito *insieme vuoto*; l'insieme vuoto si indica con il simbolo \emptyset .

Sottoinsiemi

Se A e B sono due insiemi, si dice che A è un *sottoinsieme di B* (A è *incluso in B* , A è *contenuto in B*), se ogni elemento di A è anche un elemento di B . Simbolicamente si scrive $A \subseteq B$.

Se due insiemi A e B sono descritti in modo esplicito, verificare che $A \subseteq B$ consiste nel verificare che tutti gli elementi dell'elenco di A sono contenuti anche nell'elenco di B .

Dire che A non è sottoinsieme di B (simbolicamente $A \not\subseteq B$) significa che esiste almeno un elemento di A che non è contenuto in B .

Se due insiemi A e B sono descritti in modo implicito, verificare che $A \subseteq B$ significa verificare che $P(x) \Rightarrow Q(x)$, dove $P(x)$ è il predicato che caratterizza l'insieme A e $Q(x)$ è il predicato che caratterizza l'insieme B .

Per descrivere un sottoinsieme B di un insieme A fissato si può usare una forma implicita del tipo $B = \{x \in A / P(x)\}$.

Esempio:

Definiamo con \mathbb{N} l'insieme dei **numeri naturali** (interi positivi).

Il sottoinsieme $B = \{x / \text{"x è pari"}\}$ descrive il sottoinsieme di \mathbb{N} formato dai numeri pari.

Ovviamente ogni insieme A è un sottoinsieme di A stesso ($A \subseteq A$). Un sottoinsieme B di A che non coincide con A stesso viene detto *sottoinsieme proprio* e, in questo caso, si scrive $B \subset A$.

Per convenzione si assume che l'insieme vuoto \emptyset è sottoinsieme di ogni altro insieme.

In generale, si dimostrerà che, se A è un insieme finito e contiene n elementi, i sottoinsiemi possibili di A sono in numero di 2^n . Due insiemi A e B si diranno *uguali* quando contengono gli stessi elementi e ciò equivale a dire che $A \subseteq B$ e $B \subseteq A$ (*doppia inclusione=uguaglianza*). Se $P(x)$ descrive A e $Q(x)$ descrive B , dire che A e B sono uguali equivale a dire che $P(x) \Leftrightarrow Q(x)$.

Lezione n°. 6 – 27 ott. 2000

Poiché la natura degli elementi di un insieme è assolutamente arbitraria, si possono considerare anche insiemi i cui elementi siano, a loro volta, insiemi.

Esempio:

$A = \{ \{1,2\}, \{3,5,7\} \}$ è un insieme che contiene due elementi che sono, a loro volta, insiemi.

Notare che l'insieme $\{1,2\} \in A$ ma $1 \notin A$ così come $2 \notin A$ mentre $1 \in \{1,2\}$ e $2 \in \{1,2\}$.

Fissato un insieme A , a piacere, si può costruire l'insieme di tutti i possibili sottoinsiemi di A , detto "*insieme delle parti di A* ", indicato in genere con la simbologia $\mathcal{P}(A)$.

$\mathcal{P}(A) = \{x / x \subseteq A\}$.

Esempio:

Se $A=\{a,b\}$ allora $\mathcal{P}(A)=\{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ (anche $A \subseteq A$).

La possibilità di definire insiemi di insiemi permette alcune “artificiosità”.

Consideriamo un insieme A formato da tutti gli insiemi possibili che contengono almeno 3 elementi; facendo degli esempi avremo:

$B=\{1,2,3,4\} \in A$ $C=\{a,b,c\} \in A$ $D=\{2,4\} \notin A$ (perché non contiene almeno 3 elementi).

Notare che $A \in A$ (perché, ovviamente, ha più di tre elementi, essendo un insieme infinito)

Ci sono anche casi di insiemi che non contengono se stessi. Se, ad esempio, consideriamo l'insieme A_0 formato da tutti gli insiemi che contengono esattamente 2 elementi, avremo che:

se $A_0=\{x / \text{“}x \text{ è un insieme contenente esattamente 2 elementi”}\}$ allora

$E=\{1,2\} \in A_0$ $D=\{2,4\} \in A_0$ $F=\{r,s\} \in A_0$ etc. ma $A_0 \notin A_0$ perché, essendo un insieme infinito, non contiene esattamente 2 elementi.

Questo tipo formulazioni, seguendo la teoria ingenua degli insiemi, possono creare dei *problemi*. Ad esempio, Russell costruì l'insieme Z di tutti gli insiemi che non contengono se stessi come elemento. Se consideriamo gli esempi fatti in precedenza, $A_0 \in Z$ mentre $A \notin Z$.

Il problema nasce quando si vuol determinare se Z è o non è un elemento di se stesso, perché nel momento stesso in cui affermiamo una delle due ipotesi si cade in contraddizione. Questo problema è noto come *Antinomia (o Paradosso) di Russell*.

Per evitare questi inconvenienti ci sono due soluzioni:

1. seguire la teoria assiomatica degli insiemi;
2. evitare la costruzione di insiemi del tipo “l'insieme di tutti gli insiemi...”.

In questo corso si opterà per la seconda soluzione.

Operazioni sugli insiemi.

- **Unione di insiemi**: dati due insiemi A e B si può costruire un insieme, detto *unione* ed indicato con la simbologia $A \cup B$, i cui elementi sono quelli che appartengono ad almeno uno degli insiemi A e B .

$A \cup B = \{x / x \in A \text{ oppure } x \in B\}$. L'*oppure* usato in questa formulazione è non esclusivo. Se A e B sono descritti esplicitamente, $A \cup B$ è descritto esplicitamente elencando gli elementi di A e di B (quelli comuni vanno elencati una sola volta).

Esempio:

Se $A=\{1,2,4,7\}$ e $B=\{2,3,4,8,9\}$ allora $A \cup B=\{1,2,3,4,7,8,9\}$

Notare che gli elementi 2 e 4 sono elencati una sola volta. Il numero di elementi dell'unione di due insiemi non è quindi la somma del numero degli elementi degli insiemi di partenza.

Se A e B sono descritti in maniera implicita, l'insieme $A \cup B$ si ottiene applicando la disgiunzione logica tra i predicati che definiscono i due insiemi:

Esempio:

Se $A=\{x / P(x)\}$ e $B=\{x / Q(x)\}$ allora $A \cup B=\{x / (P \vee Q)(x)\}$.

Notare la somiglianza tra i simboli di unione di insiemi e di disgiunzione logica.

- **Intersezione tra insiemi:** dati due insiemi A e B si può costruire un insieme, detto *intersezione* ed indicato con la simbologia $A \cap B$, i cui elementi sono quelli comuni all'insieme A ed all'insieme B. Se A e B non hanno elementi comuni si ha $A \cap B=\emptyset$.

$A \cap B=\{x / x \in A \text{ e } x \in B\}$.

Se A e B sono descritti esplicitamente, $A \cap B$ è descritto esplicitamente elencando gli elementi comuni di A e di B (una sola volta).

Esempio: riconsiderando gli insiemi dell'esempio precedente, avremo $A \cap B=\{2,4\}$.

Se A e B sono descritti implicitamente, l'insieme $A \cap B$ si ottiene applicando la congiunzione logica tra i predicati che definiscono i due insiemi:

Esempio: Se $A=\{x / P(x)\}$ e $B=\{x / Q(x)\}$ allora $A \cap B=\{x / (P \wedge Q)(x)\}$.

Anche in questo caso c'è una somiglianza tra i simboli di intersezione tra insiemi e di congiunzione logica.

Le operazioni di unione e di intersezione tra insiemi godono entrambe della *proprietà commutativa*: $A \cup B = B \cup A$ e $A \cap B = B \cap A$.

- **Differenza tra insiemi:** dati due insiemi A e B si può costruire un insieme, detto *differenza* ed indicato con la simbologia $A - B$, i cui elementi sono quelli di A che non sono elementi di B.

$A - B=\{x / x \in A \text{ e } x \notin B\}$

Esempio:

Se $A=\{a,b,c,e,f,r\}$ e $B=\{a,b,e,p,q\}$ allora $A - B = \{c,f,r\}$

L'operazione di differenza tra insiemi non gode della proprietà commutativa: $A-B \neq B-A$.

Nell'esempio considerato, infatti si può vedere che $B-A=\{p,q\} \neq A-B$.

Se A e B sono descritti in forma implicita l'insieme A-B si ottiene applicando l'operazione ANDNOT ai predicati che definiscono i due insiemi A e B.

Se $A=\{x / P(x)\}$ e $B=\{x / Q(x)\}$ allora $(A-B)=\{x / (P \wedge \bar{Q})(x)\}$

Esempio:

$A=\{x / \text{"x è un numero naturale } > 7\}$

$B=\{x / \text{"x è un numero naturale pari"}\}$

$A-B=\{x / \text{"x è un numero naturale } > 7 \text{ e non è pari"}\}$

$A-B=\{x / \text{"x è un numero naturale } > 7 \text{ ed è dispari"}\}$

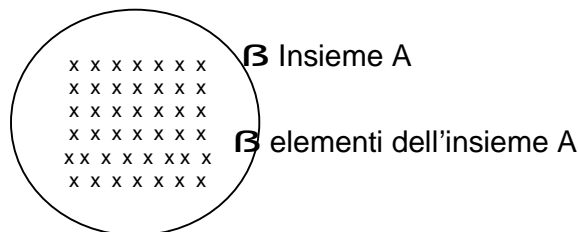
$B-A=\{x / \text{"x è un numero naturale pari ed è } \leq 7\} = \{2,4,6\}$

Si può notare che mentre A-B è un insieme infinito B-A è invece un insieme finito.

Lezione n°. 7 – 30 ott. 2000

Diagrammi di Eulero-Venn

I diagrammi di Eulero-Venn sono delle rappresentazioni grafiche di insiemi generici; un insieme viene rappresentato da una porzione di piano delimitata da una linea chiusa (spesso da una circonferenza).



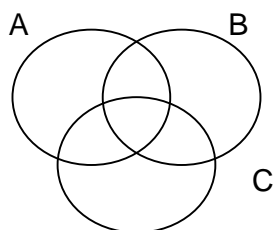
Con tali diagrammi si possono verificare alcune regole della teoria degli insiemi.

Esempio:

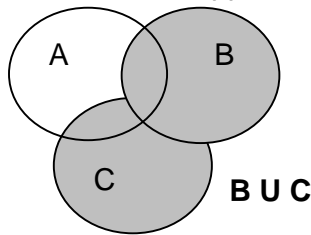
Dati gli insiemi generici A, B e C valgono le seguenti proprietà delle operazioni di unione ed intersezione (**proprietà distributive**):

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

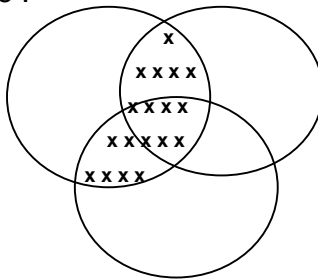
Verifichiamo la prima utilizzando i diagrammi di Eulero-Venn. Possiamo rappresentare i tre insiemi come tre circonferenze aventi eventuali parti in comune.



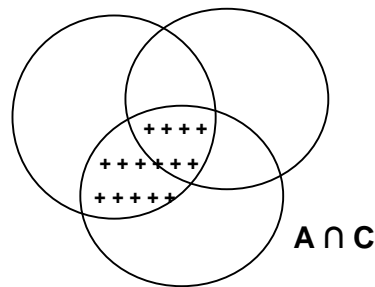
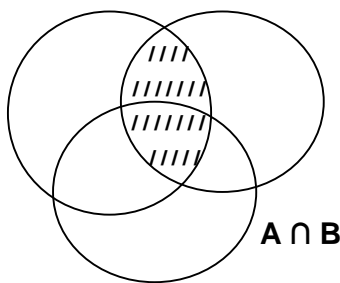
$(B \cup C)$ è dato dalle aree due circonferenze rappresentanti B e C, che distingueremo con una colorazione grigia.



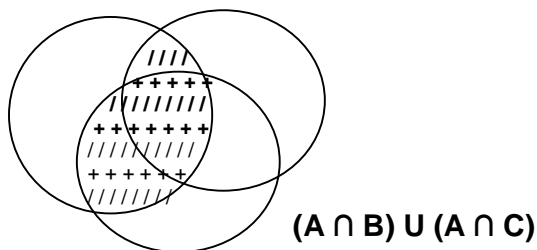
L'intersezione dell'insieme A con $(B \cup C)$ sarà dato dalla porzione di spazio comune tra la circonferenza che rappresenta A e l'insieme delle circonferenze di B e C, che distingueremo con delle crocette.



Troviamo adesso gli insiemi $(A \cap B)$ e $(A \cap C)$:



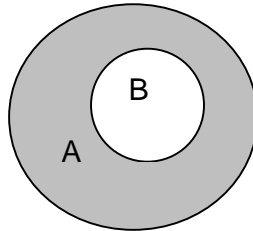
Allora, l'unione di $(A \cap B)$ ed $(A \cap C)$ sarà dato dall'unione delle due aree che abbiamo segnato con /// e +++ che, come si vede coincide con l'area che rappresenta $A \cap (B \cup C)$.



In realtà questa non è una vera e propria dimostrazione matematica ma è comunque bastevole. La seconda uguaglianza di verifica allo stesso modo, individuando prima le aree corrispondenti agli insiemi $(A \cup B)$ ed $(A \cup C)$ e poi quella corrispondente alla loro intersezione e confrontando quest'ultima con l'area corrispondente ad $A \cup (B \cap C)$.

Complementare di un insieme rispetto ad un altro.

Sia dato un insieme A ed un suo sottoinsieme B ($B \subseteq A$). Si definisce *complementare di B in A* (o *complementare di B rispetto ad A*) la differenza $A - B$, cioè l'insieme degli elementi di A che non appartengono a B . Il complementare di B in A si indica con la simbologia cB , oppure $\mathcal{A}(B)$ o, ancora, $\mathcal{C}_A(B)$ (useremo prevalentemente la prima). Utilizzando i diagrammi di Eulero-Venn, cB è individuato dall'area ombreggiata:

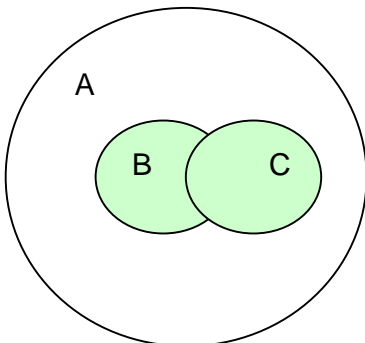


Proprietà:

1. ${}^c(B \cup C) = {}^cB \cap {}^cC$
2. ${}^c(B \cap C) = {}^cB \cup {}^cC$

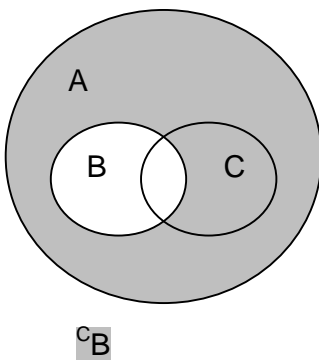
Queste proprietà sono note come **Leggi di De Morgan**.

Verifichiamo le due proprietà facendo sempre uso dei diagrammi di Eulero-Venn.

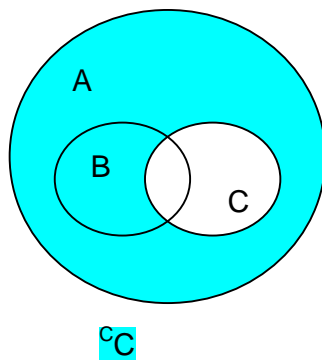


La parte colorata corrisponde a $(B \cup C)$, mentre la parte bianca interna alla circonferenza che delimita A è ${}^c(B \cup C)$.

Individuiamo adesso le aree che rappresentano cB e cC .

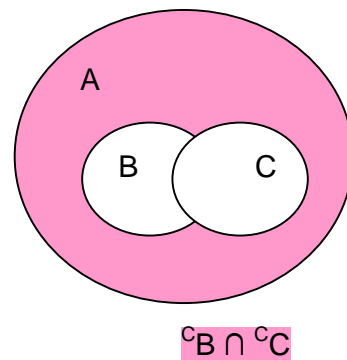


cB



cC

→



${}^cB \cap {}^cC$

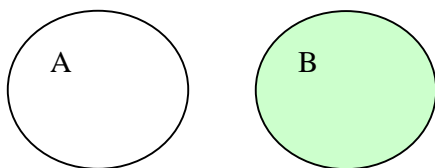
Esercizi:

1. Dati 2 insiemi A e B quando si ha che $A-B=\emptyset$ e quando si ha che $A-B=A$?
2. Dimostrare la 2^a delle proprietà distributive di unione ed intersezione e la seconda delle proprietà del complementare (utilizzando i diagrammi di Eulero-Venn).
3. Usando le operazioni di unione, intersezione e differenza, costruire, dati due insiemi A e B , un insieme che contenga gli elementi che stanno in uno solo tra A e B .
4. Se B e C sono due sottoinsiemi di A , cosa si può dire su $B \cup C$ se si sa che ${}^c B$ e ${}^c C$ non hanno elementi comuni?
5. Dire a cosa corrispondono $(A-B) \cup (B-A)$ e $(A-B) \cap (B-A)$.

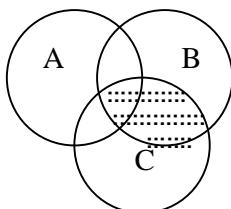
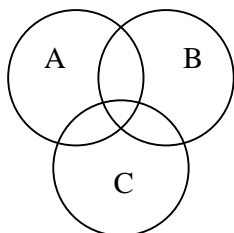
Svolgimento:

1. $A-B=\emptyset$ quando $A=B$ cioè se $A \subseteq B$ e $B \subseteq A$.

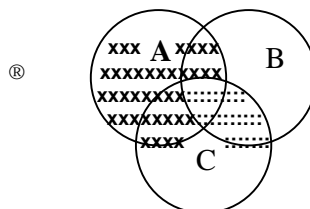
$A-B=A$ se $A \cap B=\emptyset$, cioè se i due insiemi sono disgiunti. Graficamente:



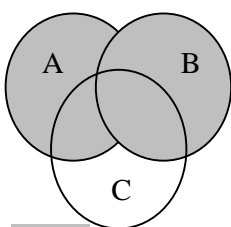
2.



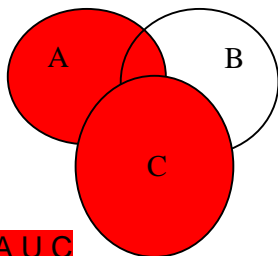
$\dots = B \cap C$



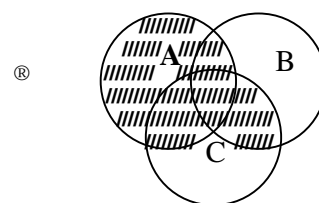
$\text{x} \dots = A \cup (B \cap C)$



$A \cup B$



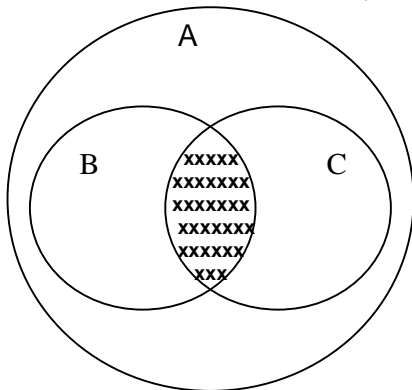
$A \cup C$



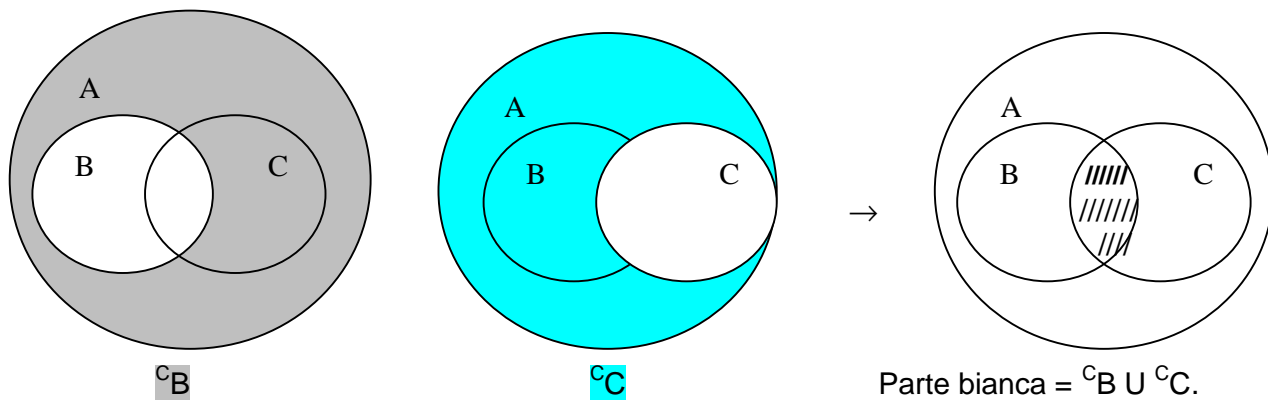
$\text{////} = (A \cup B) \cap (A \cup C)$

Come si vede le due aree coincidono per cui $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Verifichiamo adesso che ${}^c(B \cap C) = {}^cB \cup {}^cC$.



La parte segnata con xxxx è $B \cap C$ quindi tutta la parte bianca è ${}^c(B \cap C)$.



Confrontando le due aree si verifica la validità della 2^a legge di De Morgan.

3. L'insieme degli elementi che stanno o in A o in B è dato da: $(A-B) \cup (B-A)$.
4. Che B e C sono uguali.
5. $(A-B) \cup (B-A)$ corrisponde all'insieme che comprende gli elementi che stanno o in A o in B (OR ESCLUSIVO).
 $(A-B) \cap (B-A)$ coincide invece con l'insieme vuoto.

Lezione n°. 8 – 6 nov. 2000

Aritmetica degli interi relativi.

Si definisce con \mathbb{Z} l'insieme dei numeri interi relativi: $\mathbb{Z}=\{0,1,-1,2,-2,\dots\}$.

Si definisce \mathbb{N} l'insieme dei numeri naturali: $\mathbb{N}=\{1,2,3,\dots\}$.

Si presumono noti i seguenti concetti:

1. le operazioni di somma e prodotto fra numeri interi (si intendono *somma* e *prodotto* nel senso più ampio, al limite con un solo addendo o un solo fattore);
2. le proprietà di somma e prodotto (associativa, commutativa, distributiva);
3. il concetto di *minore*, *minore ed uguale* e le relative proprietà.

Si aggiunge un ulteriore assioma:

Assioma del buon ordinamento dei numeri naturali:

dato un qualsiasi sottoinsieme S , non vuoto, dell'insieme dei numeri naturali \mathbb{N} , esiste sempre in S un numero minimo $s \in S$ (cioè tale che non esiste, nel sottoinsieme S , un elemento minore di s).

Principio di induzione.

Se A è un insieme finito contenente 3 elementi, $A = \{a, b, c\}$, i suoi sottoinsiemi sono:

$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\} = A$ (sono in numero di $8 = 2^3$).

Se A è un insieme finito contenente 4 elementi, $A = \{a, b, c, d\}$, i suoi sottoinsiemi sono:

$\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, \{a, b, d\}, \{b, c, d\}, \{a, b, c, d\} = A$ (sono in numero di $16 = 2^4$).

Sembra allora che sia vero il seguente teorema:

se A è un qualunque insieme finito e non vuoto con n elementi, il numero dei suoi sottoinsiemi è 2^n .

In pratica si ha il predicato $P(n) = \text{"Se } A \text{ è un insieme finito non vuoto con } n \text{ elementi, i sottoinsiemi di } A \text{ sono in numero di } 2^n\text{"}$ con campo di variabilità \mathbb{N} .

Il teorema equivale a dire che $P(n)$ è vero per ogni valore della variabile n . Si è già verificato il predicato $P(n)$ per i valori 3 e 4, cioè $P(3)$ e $P(4)$ sono proposizioni vere. Il problema da affrontare è il fatto che i valori che la variabile n può assumere sono infiniti per cui non è possibile verificare $P(n)$ per tutti i valori possibili di n . Una soluzione a questo problema è data dal **principio di induzione**, il cui enunciato è il seguente:

Sia $P(n)$ un predicato della variabile n , con campo di variabilità l'insieme dei numeri naturali \mathbb{N} ; se sono verificate le 2 ipotesi:

1. il predicato è vero per $n=1$, cioè $P(1)$ è vera;
2. ogni volta che il predicato è vero per un certo valore $n=k$ della variabile ed esso è vero anche per il valore successivo $n=k+1$;

allora il predicato $P(n)$ è vero per ogni valore della variabile n (all'interno del campo di variabilità \mathbb{N}).

Dimostrazione:

Procediamo per assurdo: se la tesi fosse falsa, vorrebbe dire che esiste almeno un valore della variabile n per cui $P(n)$ è una proposizione falsa. Costruiamo allora un insieme che raccolga tali valori di n : $S = \{t / t \in \mathbb{N} \text{ e } P(t) \text{ è falso}\}$.

Si ha che $S \subseteq \mathbb{N}$ ed $S \neq \emptyset$. Per l'assioma del buon ordinamento dei numeri naturali, esisterà almeno un numero minimo $s \in S$; allora $s \in \mathbb{N}$ e $P(s)$ è una proposizione falsa. Per l'ipotesi n°. 1 il predicato è vero per $n=1$ e quindi $s \neq 1$. Allora siamo giunti alla conclusione che $s \in \mathbb{N}$ ed $s \neq 1$, quindi $s > 1$, cioè $(s-1) > 0$, quindi $(s-1)$ è un numero intero positivo, ossia $(s-1) \in \mathbb{N}$. Ma $s \in S$ è il minimo numero di S , quindi $(s-1) \notin S$ (perché $s-1 < s$). Per come è stato costruito l'insieme S , si deduce che il predicato $P(n)$ è vero per il valore $n=(s-1)$, cioè $P(s-1)$ è una proposizione vera. Per l'ipotesi n°. 2 il predicato sarà allora vero anche per il valore successivo, ma il valore successivo di $(s-1)$ è $(s-1)+1=s$ e noi abbiamo ipotizzato, per assurdo, che $P(s)$ sia falso. Siamo allora caduti in contraddizione per cui il Principio di induzione è verificato.

Lezione n°. 9 – 8 nov. 2000

Tornando all'esempio introduttivo, dimostriamo, utilizzando il principio di induzione, che $P(n)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto A con n elementi è 2^n " è vero per ogni valore di n .

Dovremo verificare i due punti del principio di induzione:

1. $P(1)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto A con 1 elemento è $2^1=2$ " è una proposizione vera perché i sottoinsiemi di $A=\{a\}$ sono \emptyset e $\{a\}=A$.
2. $P(k)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto A con k elementi è 2^k ".
 $P(k+1)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto A con $(k+1)$ elementi è 2^{k+1} ".

Sapendo che $P(k)$ è una proposizione vera, dobbiamo verificare che lo è anche $P(k+1)$. Sia dato l'insieme $A=\{a_1, a_2, a_3, \dots, a_k, a_{k+1}\}$ con $(k+1)$ elementi e consideriamo l'insieme differenza $A-\{a_{k+1}\}=\{a_1, a_2, a_3, \dots, a_k\}$. Questo insieme è formato da k elementi e quindi sappiamo per ipotesi che i suoi sottoinsiemi sono in numero di 2^k .

Ora, i sottoinsiemi di A si possono dividere in due categorie:

1. i sottoinsiemi che non contengono l'elemento a_{k+1} ;
2. i sottoinsiemi che contengono l'elemento a_{k+1} .

Contiamo adesso i sottoinsiemi di queste due categorie: quelli della prima coincidono con i sottoinsiemi di $A - \{a_{k+1}\}$ che sappiamo essere in numero di 2^k ; quelli della seconda categoria si ottengono aggiungendo a ciascun sottoinsieme della prima l'elemento a_{k+1} e quindi sono sempre in numero di 2^k . Allora il numero totale dei sottoinsiemi di A è : $2^k + 2^k = 2 * 2^k = 2^1 * 2^k = 2^{k+1}$.

Abbiamo allora verificato che se è vera la proposizione $P(k)$ lo è anche $P(k+1)$, quindi tutte le condizioni del principio di induzione sono valide per cui possiamo dire che il predicato $P(n)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto A con n elementi è 2^n " è vero per ogni valore di n.

Esempi:

1) consideriamo la somma dei primi 4 numeri naturali $1+2+3+4=10$ e la somma dei primi 6 numeri naturali $1+2+3+4+5+6=21$. Possiamo notare che:

$$1+2+3+4=(4*5)/2 \quad \text{e} \quad 1+2+3+4+5+6=(6*7)/2.$$

Sembra allora che sia vero per ogni valore di n il predicato

$P(n)$ ="la somma dei primi n numeri naturali è uguale a $(n*(n+1))/2$ " cioè $1+2+3+...+n=(n*(n+1))/2$.

Si è già verificato che le proposizioni $P(4)$ e $P(6)$ sono vere. Utilizzando il principio di induzione dobbiamo verificare che $P(n)$ è vero per ogni valore di n.

1. $P(1)$ ="la somma dei primi 1 numeri naturali è $1=(1*(1+1))/2=2/2=1$ " è vera.
2. sapendo che $P(k)$ è vera dovremo dimostrare che $P(k+1)$ è anch'essa vera:

$$P(k)$$
="1+2+3+...+k=(k*(k+1))/2"

$$P(k+1)$$
="1+2+3+...+k+(k+1)=((k+1)*(k+1+1))/2=((k+1)*(k+2))/2.

Dobbiamo dimostrare in pratica l'uguaglianza:

$$1+2+3+...+k+(k+1)=((k+1)*(k+2))/2.$$

Essendo $P(k)$ una proposizione vera possiamo riscrivere l'uguaglianza nel seguente modo: $(k*(k+1))/2 + (k+1)=((k+1)*(k+2))/2$.

$(k*(k+1))/2 + (k+1)=(k(k+1)+2(k+1))/2=((k+1)*(k+2))/2$ che rende vera la proposizione $P(k+1)$ e quindi, per il principio di induzione, il predicato $P(n)$ per ogni valore di $n \in \mathbb{N}$.

Esercizio 1.

Dimostrare che la somma dei primi n quadrati dei numeri naturali è:

$$1^2+2^2+\dots+n^2=\frac{1}{6}n(n+1)(2n+1).$$

Svolgimento:

$P(n)=1^2+2^2+\dots+n^2=\frac{1}{6}n(n+1)(2n+1)$. Utilizziamo il principio di induzione:

1. $P(1)=1^2=\frac{1}{6}\cdot 1(1+1)(2\cdot 1+1) \rightarrow 2=\frac{1}{6}\cdot 2\cdot 3 \rightarrow 2=\frac{1}{6}\cdot 6=2 \Rightarrow P(1)$ è vera.

2. $P(k)=1^2+2^2+\dots+k^2=\frac{1}{6}k(k+1)(2k+1)$

$$P(k+1)=1^2+2^2+\dots+k^2+(k+1)^2=\frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)=\frac{1}{6}(k+1)(k+2)(2k+3)$$

Essendo, da $P(k)$, $1^2+2^2+\dots+k^2=\frac{1}{6}k(k+1)(2k+1)$ nella espressione di $P(k+1)$ possiamo sostituire al primo membro alla somma dei primi k termini l'espressione $\frac{1}{6}k(k+1)(2k+1)$ ed otteniamo:

$$\frac{1}{6}k(k+1)(2k+1) + (k+1)^2 = \frac{1}{6}(k+1)(k+2)(2k+3) \quad \text{dividendo ambo i membri per } (k+1) \text{ si ha:}$$

$$\frac{1}{6}k(2k+1) + (k+1) = \frac{1}{6}(k+2)(2k+3) \quad \text{e sviluppando le somme ed i prodotti:}$$

$$\frac{1}{6}(2k^2+k+6k+6) = \frac{1}{6}(2k^2+3k+4k+6) \rightarrow \frac{1}{6}(2k^2+7k+6) = \frac{1}{6}(2k^2+7k+6)$$

abbiamo quindi dimostrato che se $P(k)$ è vera lo è anche $P(k+1)$ e quindi, per il principio di induzione, che l'uguaglianza $1^2+2^2+\dots+n^2=\frac{1}{6}n(n+1)(2n+1)$ è vera per ogni $n \in \mathbb{N}$.

Esercizio 2.

a) dimostrare che, elencando i primi numeri naturali dispari, quello di posto n è $(2n-1)$;

b) Dimostrare che la somma dei primi n numeri naturali dispari coincide con n^2 .

Per dimostrare la b) utilizzare la a).

Svolgimento:

a) utilizziamo il principio di induzione:

$P(n)$ = "elencando i primi n numeri naturali dispari, l'elemento di posto n è uguale a $(2n-1)$."

$P(1)$: l'elemento di posto 1 nella successione è 1 e si ha $1=2 \cdot 1 - 1 = 1 \Rightarrow P(1)$ è vera.

$P(k)$: se x è l'elemento di posto k nella successione avremo che $x=2k-1$

$P(k+1)$: il numero dispari successivo a x è $x+2$, quindi avremo:

$$x+2=2(k+1)-1=2k+2-1=(2k-1)+2.$$

Da $P(k)$ sappiamo che $(2k-1)=x$ quindi possiamo operare una sostituzione nel secondo membro dell'espressione $P(k+1)$ ed otterremo: $x+2=x+2$, e quindi per il principio di induzione $P(n)$ è vero per ogni valore di $n \in \mathbb{N}$.

b) $P(n)$ ="la somma dei primi n numeri naturali dispari coincide con n^2 ".

$P(1)$: l'elemento di posto 1 è 1 per cui abbiamo $1=1^2$.

$P(k)$: se chiamiamo x l'elemento di posto k nella sommatoria, avremo:

$$1+3+5+\dots+x=k^2;$$

$P(k+1)$: l'elemento di posto $(k+1)$ nella sommatoria sarà $(x+2)$ quindi abbiamo:

$$1+3+5+\dots+x+(x+2)=(k+1)^2.$$

Da quanto dimostrato al punto a) possiamo sostituire ad x l'espressione $(2k-1)$, essendo x l'elemento di posto k nella successione dei numeri naturali dispari:

$1+3+5+\dots+(2k-1)+(x+2)=(k+1)^2$ che possiamo riscrivere nel seguente modo:

$$1+3+5+\dots+x+(2k-1+2)=(k+1)^2 \rightarrow 1+3+5+\dots+x+(2k+1)=(k+1)^2 \text{ ed ancora, in base a}$$

$P(k)$, possiamo sostituire la parte di polinomio evidenziata con k^2 :

$k^2+2k+1=(k+1)^2$; osservando il primo membro dell'uguaglianza si nota subito che esso altro non è che lo sviluppo del quadrato del binomio $(k+1)$ per cui abbiamo $(k+1)^2=(k+1)^2$, e quindi, per il principio di induzione possiamo dire che $P(n)$ è vero per ogni valore di $n \in \mathbb{N}$.

Osservazione sul principio di induzione.

Se nell'enunciato del principio di induzione si sostituisce il numero 1 (base dell'induzione) con un qualunque numero naturale n_0 , si ottiene un altro enunciato noto come

Principio di induzione generalizzato:

Sia $P(n)$ un predicato con n che assume valori naturali, se:

1. $P(n)$ è vero per il valore $n=n_0$;
2. ogni volta che $P(n)$ è vero per un valore $k \geq n_0$ $P(n)$ è vero anche per il successivo $n=k+1$,
allora $P(n)$ è vero per ogni valore di $n \geq n_0$.

Nota: cambia la base del principio di induzione e, in pratica, si opera una limitazione che può essere utile in quei casi in cui un predicato è vero per valori da un certo n_0 in su. La dimostrazione è uguale a quella vista con base uguale ad 1.

Esempio:

Consideriamo il predicato $P(n)$ ="il quadrato del numero naturale n è maggiore di 10".

$P(1), P(2), P(3)$ non sono proposizioni vere ma $P(4), P(5)$ etc. lo sono, sembra cioè che $P(n)$ sia vero per ogni valore di $n \geq 4$. Utilizzando il principio di induzione generalizzato, con base $n_0=4$, possiamo vedere se ciò è vero.

1. $P(4)$ è vero, infatti $4^2=16>10$;
2. preso un valore $n=k \geq 4$, sapendo che $P(k)$ è vera dobbiamo verificare se lo è anche $P(k+1)$.

Sapendo che $k^2 > 10$, dovremo dimostrare che $(k+1)^2 > 10$.

$(k+1)^2 = k^2 + 2k + 1$, essendo $k \in \mathbb{N}$, la quantità $(2k+1)$ è sicuramente positiva; visto che $k^2 > 10$ a maggior ragione lo sarà allora $k^2 + (2k+1) = (k+1)^2$ cioè $(k+1)^2 > 10$.

Per il principio di induzione generalizzato, possiamo allora affermare che

$P(n)$ ="il quadrato del numero naturale n è maggiore di 10" è vero per ogni valore di n tale che $n \geq 4$.

Lezione n°. 10 – 10 nov. 2000

Osservazione: si sa che, per l'assioma del buon ordinamento, ogni insieme non vuoto costituito da numeri naturali ha sempre un numero minimo; ciò vale anche per un insieme non vuoto che, oltre a numeri naturali, contenga anche l'elemento zero. Se un insieme non vuoto contiene numeri naturali con l'aggiunta dello zero, quest'ultimo è il minimo dell'insieme stesso. Se invece lo zero non è presente siamo sempre nei casi previsti dall'assioma del buon ordinamento. Si potrebbe chiamare questa estensione *assioma del buon ordinamento generalizzato*.

Algoritmo della divisione per i numeri interi.

Dati comunque due interi $a \geq 0$ (detto *dividendo*) e $b > 0$ (detto *divisore*) esistono sempre due numeri interi $q \geq 0$ (*quoziente*) ed $r \geq 0$ (*resto*) tali che $a = b \cdot q + r$ con $r < b$.

Dimostrazione: la tesi è l'esistenza dei numeri interi q ed r con tutte le proprietà richieste.

Consideriamo le seguenti differenze:

$a-b*0, a-b*1, a-b*2, \dots, a-b*t$ che costituiscono l'insieme infinito delle differenze nella forma $a-b*t$, con t numero intero e $t \geq 0$. Tali differenze sono degli interi relativi (positivi, negativi o nulli). Raccogliamo ora in un insieme S solo le differenze che sono ≥ 0 :

$$S = \{x / x = a - b*t \text{ con } t \text{ intero } \geq 0 \text{ ed } x \geq 0\}.$$

Certamente $S \neq \emptyset$ perché almeno la differenza $a-b*0=a$ appartiene all'insieme S (essendo $a \geq 0$). Per l'assioma del buon ordinamento (generalizzato), esiste in S un numero minimo $s \in S$. Osserviamo le qualità del numero $s \in S$: s è una delle differenze che abbiamo considerato, quindi ha la forma $s = a - b*t$, con t intero ≥ 0 ed inoltre $s \geq 0$ (visto che abbiamo costruito l'insieme S con le differenze non negative). Allora possiamo scrivere $a = b*t + s$.

Si sono allora trovati due numeri s e t che hanno tutte le caratteristiche del quoziente e del resto tranne per il fatto che non sappiamo se $r = s < b$. Cerchiamo di dimostrarlo; procedendo per assurdo, neghiamo che $r = s < b$. Se fosse $r = s \geq b$ avremmo $s - b \geq 0$, quindi la differenza $(s - b)$ sarebbe un numero intero non negativo e, ricordando che s , per come è stato definito l'insieme S cui appartiene, è una differenza della forma $s = a - b*t$. Combinando le due formule si otterrebbe:

$$(a - b*t) - b = a - b(t+1) \geq 0 \quad \text{con } (t+1) \text{ intero } \geq 0 \quad \text{e} \quad s - b \geq 0.$$

Da ciò si dedurrebbe che $(s - b) \in S$ ma $(s - b) < s$ (perché $b > 0$) quindi avremmo trovato un numero minore di s nell'insieme S di cui s è il minimo; negando che $r = s < b$ arriviamo quindi ad una contraddizione per cui anche l'ultima caratteristica richiesta per la coppia q ed s è provata e l'enunciato dell'algoritmo della divisione per i numeri interi è dimostrato.

Da un punto di vista pratico, per trovare il quoziente q ed il resto r di una divisione tra numeri interi si può anche usare l'algoritmo classico:

$$\begin{array}{r|l} a & b \\ r & q \end{array}$$

che è sì più facile per un calcolo manuale, ma risulta di difficile implementazione in un calcolatore. Riguardando la dimostrazione del teorema trattato, si può notare che il resto $r = s$ è la più piccola differenza non negativa tra quelle del tipo $(a - b*t)$ con t intero ≥ 0 , per cui si può ricavare un algoritmo, facilmente implementabile in un calcolatore, che consiste nel calcolare le differenze:

$$a - b*0 = a$$

$$a - b*1 = a - b$$

$$a - b*2 = (a - b) - b = a - 2b$$

$$a - b*3 = (a - 2b) - b \quad \text{etc.}$$

eseguire un controllo sul segno di ognuna di esse e bloccando l'iterazione al passo precedente la prima differenza di segno negativo: tale differenza fornisce il resto mentre il numero d'ordine della differenza fornisce il quoziente.

Lezione n°. 11 – 13 nov. 2000

Scrittura di un numero intero $a \geq 0$ in base $b > 1$.

È un'applicazione del teorema dell'algoritmo della divisione per i numeri interi.

Fissiamo un numero intero $a \geq 0$ ed un intero $b > 1$ (detto "base") ed usiamo l'algoritmo della divisione con a come dividendo e b come divisore: esisteranno allora due interi q_0 ed r_0 , entrambi ≥ 0 tali che $a = b \cdot q_0 + r_0$, con $r_0 < b$. Se il quoziente $q_0 \neq 0$ (cioè $q_0 > 0$) operiamo un'altra divisione, prendendo q_0 come dividendo e b come divisore: esistono allora due interi q_1 ed r_1 , entrambi ≥ 0 , tali che $q_0 = b \cdot q_1 + r_1$, con $r_1 < b$. Ancora, se il quoziente $q_1 \neq 0$ (cioè $q_1 > 0$), possiamo operare una nuova divisione, prendendo q_1 come dividendo e b come divisore, trovando che esistono due interi q_2 ed r_2 , entrambi ≥ 0 tali che $q_1 = b \cdot q_2 + r_2$, con $r_2 < b$; se $q_2 \neq 0$ ($q_2 > 0$) si ripete ancora il procedimento etc.

Dimostriamo che questo procedimento ha un termine, cioè che per una certa divisione si ottiene un quoziente uguale a zero. Osserviamo che il quoziente di ogni divisione è minore del quoziente della divisione precedente: infatti, essendo $b > 1$, si ha che $b \cdot q_1 > q_1$, ed essendo $r_1 \geq 0$, si ha $q_0 = b \cdot q_1 + r_1 \geq b \cdot q_1 > q_1$, quindi $q_0 > q_1$. Analogamente si dimostra che $q_2 > q_1$, che $q_3 > q_2$ etc. Se, per assurdo, le divisioni successive non avessero mai termine, avremmo un insieme S di numeri interi > 0 (numeri naturali) formato dai quozienti $q_0 > q_1 > q_2 > q_3 > \dots$ che non avrebbe un minimo (visto che si sta supponendo che ad ogni divisione successiva si trova un quoziente minore del precedente) e questo sarebbe in contraddizione con l'assioma del buon ordinamento. Possiamo quindi affermare che esiste un quoziente $q_n = 0$.

Elenchiamo le divisioni che abbiamo effettuato:

$$a = b \cdot q_0 + r_0$$

$$q_0 = b \cdot q_1 + r_1$$

$$q_1 = b \cdot q_2 + r_2$$

$$q_2 = b \cdot q_3 + r_3$$

.....

$$q_{n-1} = b \cdot q_n + r_n \quad \text{con } q_n = 0.$$

Operando delle sostituzioni successive si ottiene:

$$a = b \cdot q_0 + r_0 = b(b \cdot q_1 + r_1) + r_0 = b^2 \cdot q_1 + b \cdot r_1 + r_0 = b^2(b \cdot q_2 + r_2) + b \cdot r_1 + r_0 = b^3 \cdot q_2 + b^2 \cdot r_2 + b \cdot r_1 + r_0 = \dots \dots \dots \\ \dots \dots \dots = b^n \cdot q_{n-1} + b^{n-1} \cdot r_{n-1} + \dots + b^2 \cdot r_2 + b \cdot r_1 + r_0 = b^n \cdot r_n + b^{n-1} \cdot r_{n-1} + \dots + b^2 \cdot r_2 + b \cdot r_1 + r_0$$

La scrittura ottenuta:

$a = r_n \cdot b^n + r_{n-1} \cdot b^{n-1} + \dots + r_2 \cdot b^2 + r_1 \cdot b + r_0$ è detta **scrittura di a in base b** ed i numeri $r_0, r_1, r_2, \dots, r_n$ sono detti *cifre* della scrittura. Tali numeri sono tutti numeri interi ≥ 0 e tutti $< b$, cioè i possibili valori delle cifre sono compresi nell'intervallo $[0..b-1]$.

La simbologia usata è $a = (r_n r_{n-1} r_{n-2} \dots r_2 r_1 r_0)_b$.

Esempio:

Scrivere il numero $a=121$ in base $b=3$.

Le cifre saranno comprese tra 0 e 2 (0,1,2). Procedendo con l'algoritmo visto otteniamo:

1^a divisione: $121 = 3 \cdot 40 + 1$ dove $121=a$, $3=b$, $40= q_0$, $1=r_0$;

2^a divisione: $40 = 3 \cdot 13 + 1$ dove $40=q_0$, $3=b$, $13=q_1$, $1=r_1$;

3^a divisione: $13 = 3 \cdot 4 + 1$ dove $13=q_1$, $3=b$, $4=q_2$, $1=r_2$;

4^a divisione: $4 = 3 \cdot 1 + 1$ dove $4=q_2$, $3=b$, $1=q_3$, $1=r_3$;

5^a divisione: $1 = 3 \cdot 0 + 1$ dove $1=q_3$, $3=b$, $0=q_4$, $1=r_4$.

Allora $a=121=(11111)_3$. (che le cifre siano tutte =1 è un caso).

Il procedimento inverso si effettua applicando la formula della scrittura vista e quindi effettuando le moltiplicazioni delle singole cifre per le potenze della base (relative alla posizione della base stessa) e sommando i prodotti:

Esempio:

Trovare il corrispondente numero intero al numero $(10241)_5$.

$$(10241)_5 = 1 \cdot 5^4 + 0 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5^1 + 1 \cdot 5^0 = 625 + 0 + 50 + 20 + 1 = 696.$$

Particolari basi sono la base $b=10$ (*decimale*), che è quella usata comunemente (forse in relazione al numero di dita delle mani) e la base $b=2$ (*binaria*), le cui cifre sono 0 ed 1 e che si utilizza per implementare i numeri nei calcolatori in quanto si può trovare una corrispondenza con gli stati dei circuiti (alta o bassa tensione).

Lezione n°. 12 – 15 nov. 2000

Divisori e multipli.

Dati due numeri interi positivi a e b , si dice che b è un *divisore di a* (oppure che a è *multiplo di b*), e si scrive simbolicamente $b|a$, se esiste un numero intero $c>0$ tale che $b*c=a$. Se tale numero c non esiste si dice che b non è *divisore di a* (a non è *multiplo di b*) e si scrive simbolicamente $b \nmid a$. Per verificare se è vero che $b|a$, si può usare l'algoritmo della divisione (dati due interi $a \geq 0$ e $b > 0$, esistono due interi q ed r , entrambi ≥ 0 , tali che $a=b*q+r$, con $r < b$), prendendo in esame il resto r della divisione tra a (dividendo) e b (divisore); se $r=0$ si ha $a=b*q$ (ovviamente $q>0$ perché lo sono sia a che b) e quindi possiamo concludere che $b|a$. Se invece $r \neq 0$ (quindi $r > 0$) allora $b \nmid a$ perché se, per assurdo, fosse $b|a$ allora esisterebbe un intero $c>0$ tale che $b*c=a$. Allora, sotto l'ipotesi $r \neq 0$ avremmo le due uguaglianze: $a=b*q+r$ ed $a=b*c$, dalle quali si otterrebbe:

$r=a-b*q=b*c-b*q=b*(c-q)$ e poiché r e b sono entrambi >0 , anche la quantità $(c-q)$ dovrebbe essere >0 ed essendo un intero ≥ 1 (in quanto differenza di due interi) moltiplicando b per una quantità positiva ≥ 1 , otterremmo un numero maggiore di b , cosa che ci fa cadere in contraddizione perché, per la definizione stessa del resto r , deve essere $r < b$.

Numeri primi.

Se a è un qualunque numero intero >0 , dall'identità $a=a*1$ si ottiene che i numeri 1 ed a sono divisori di a ; essi sono detti *divisori banali*.

Un numero intero $a>0$ si dice **primo** se $a \neq 1$ e se a ha solo i divisori banali (cioè gli unici divisori di a sono 1 ed a stesso).

Osservazione: l'esclusione del numero 1 dall'insieme dei numeri primi sarà chiarita in seguito con il Teorema di fattorizzazione unica.

Come fare a verificare se un numero intero $a>0$ è primo oppure no? Si potrebbe seguire un metodo immediato, verificando se tutti i numeri compresi strettamente tra 1 ed a (cioè esclusi gli estremi che sono i divisori banali) sono oppure no divisori di a , ma questo metodo risulta poco efficiente e lungo. Esiste un metodo più efficiente basato sull'osservazione che, se un divisore non banale di a esiste, allora esiste anche un divisore non banale di a che è $\leq \sqrt{a}$ (perché se $a=b*c$, non si può avere contemporaneamente $b > \sqrt{a}$ e $c > \sqrt{a}$, perché altrimenti sarebbe $a=b*c > \sqrt{a} * \sqrt{a} = a$, che è

una contraddizione) e quindi ci si può limitare, nella ricerca dei divisori non banali di a , a tutti i numeri $\leq \sqrt{a}$.

Esempio:

se $a=113$, poiché $\sqrt{a} \cong 10$ è di poco superiore a 10, ci si può limitare alla verifica sui numeri ≤ 10 (e >1), cioè (2,3,4,5,6,7,8,9,10). Essendo $a=113$ un numero dispari possiamo subito scartare i numeri pari, utilizzando i criteri di divisibilità si vede che nessuno degli altri numeri è divisore di 113 che quindi è un numero primo.

Un obbiettivo della ricerca matematica attuale è trovare algoritmi sempre più efficienti per verificare se un numero è primo oppure no. L'importanza dei numeri primi è relativa al loro uso come base della crittografia (scienza che studia la cifratura e la decifratura di messaggi).

Massimo comune divisore.

Siano dati due numeri a e b entrambi >0 . Si dice che un numero intero $d>0$ è il massimo comune divisore di a e b (si scrive $d=m.c.d.(a,b)$), se:

1. $d|a$ e $d|b$ (cioè d è un divisore comune di a e b);
2. se d_0 è un qualunque altro divisore comune di a e b , si deve avere $d_0|d$ (cioè d è multiplo di ogni altro divisore comune di a e b);

Il secondo punto ci dice che d è il più grande dei divisori comuni di a e b .

Il problema da risolvere è: chi ci assicura che un tale numero intero positivo d esiste?

Questo viene assicurato dal seguente

Teorema:

dati due numeri interi a e b , entrambi >0 , esiste sempre un loro massimo comune divisore.

Dimostrazione:

si userà l'assioma del buon ordinamento. Diamo prima una definizione: si definisce *combinazione lineare* di a e b un numero intero relativo (positivo, negativo o nullo) della forma $(a*x+b*y)$, con x e y numeri interi relativi (esempi di combinazioni lineari sono: $a*2+b*3$, $a*(-2)+b*(-5)$ etc.); i numeri x e y sono detti *coefficienti* della combinazione lineare. Costruiamo adesso l'insieme S delle combinazioni lineari di a e b che sono positive: $S=\{z / z=a*x+b*y, \text{ con } x \text{ e } y \text{ interi relativi e } z>0\}$.

Possiamo affermare che $S \neq \emptyset$ perché, essendo $a=a*1+b*0$ ed $a>0$, a è una combinazione lineare di a e b e lo stesso si può dire per b , quindi $a \in S$ e $b \in S$. Per l'assioma del buon ordinamento esiste allora un elemento minimo in S , che chiameremo d . Dimosteremo che

$d = \text{m.c.d.}(a, b)$, verificheremo cioè che esso gode delle proprietà del massimo comune divisore.

1. deve essere divisore comune di a e b : usando l'algoritmo della divisione prendendo a come dividendo e d come divisore, esisteranno due numeri interi q ed r , entrambi ≥ 0 , tali che $a = d \cdot q + r$, con $r < d$; per verificare che $d|a$, dobbiamo verificare che r sia uguale a zero: se, per assurdo, fosse $r \neq 0$ (cioè $r > 0$) si osserva che, essendo $d \in S$, esso sarà una combinazione lineare di a e b , nella forma $d = a \cdot x + b \cdot y$, con x e y interi relativi; dalle due uguaglianze $a = d \cdot q + r$ e $d = a \cdot x + b \cdot y$, ricavando r e sostituendo, otteniamo:

$$r = a - d \cdot q = a - (a \cdot x + b \cdot y) \cdot q = a \cdot (1 - x \cdot q) + b \cdot (-y \cdot q)$$

essendo $(1 - x \cdot q)$ e $(-y \cdot q)$ due numeri interi relativi, avremmo ottenuto che r è una combinazione lineare di a e b ed essendo anche $r > 0$ risulterebbe allora $r < d$; ma d è il minimo di S e quindi siamo in contraddizione.

2. se d_0 è un divisore comune di a e b , deve verificarsi anche $d_0|d$; osserviamo che, in effetti, se d_0 è un divisore comune di a e b , allora esistono due numeri interi c ed f , entrambi > 0 , tali che $a = d_0 \cdot c$ e $b = d_0 \cdot f$; ricordando che d è della forma $d = a \cdot x + b \cdot y$, con x e y interi relativi, possiamo scrivere:

$$d = a \cdot x + b \cdot y = (d_0 \cdot c) \cdot x + (d_0 \cdot f) \cdot y = d_0 \cdot (c \cdot x + f \cdot y)$$

essendo la quantità $(c \cdot x + f \cdot y)$ un numero intero, si deduce che $d_0|d$.

Verificate le due proprietà di d , possiamo affermare che esiste sempre un massimo comune divisore tra due numeri interi positivi.

Lezione n°. 13 – 17 nov. 2000

Dati due numeri interi a e b , entrambi > 0 , si è definito massimo comune divisore di a e b quell'intero d che ha le proprietà:

1. $d|a$ e $d|b$;
2. d è multiplo di tutti i divisori comuni di a e b .

Osservazione: nel corso della dimostrazione del teorema che assicura l'esistenza del massimo comune divisore tra due numeri interi positivi, si è notato che d si può scrivere come combinazione lineare di a e b , cioè $d = a \cdot x + b \cdot y$, con x e y opportuni interi relativi.

Si pongono adesso due problemi;

1. trovare un algoritmo di calcolo per calcolare il m.c.d.;
2. trovare un algoritmo di calcolo per poter calcolare i coefficienti x e y della combinazione lineare $a \cdot x + b \cdot y = d$.

I due problemi possono essere risolti con l'**Algoritmo di Euclide** (delle divisioni successive).

Siano dati due interi a e b , entrambi >0 ; usiamo l'algoritmo della divisione prendendo a come dividendo e b come divisore: esistono allora due interi ≥ 0 , q_1 ed r_1 , tali che $a=b*q_1+r_1$, con $r_1 < b$.

Se $r_1 \neq 0$ (cioè $r_1 > 0$), operiamo un'altra divisione prendendo b come dividendo ed r_1 come divisore: esistono allora due interi ≥ 0 , q_2 ed r_2 , tali che $b=r_1*q_2+r_2$, con $r_2 < r_1$.

Se $r_2 \neq 0$ (cioè $r_2 > 0$), operiamo un'altra divisione prendendo r_1 come dividendo ed r_2 come divisore: esistono allora due interi ≥ 0 , q_3 ed r_3 , tali che $r_1=r_2*q_3+r_3$, con $r_3 < r_2$.

Se $r_3 \neq 0$ (cioè $r_3 > 0$), operiamo un'altra divisione prendendo r_2 come dividendo ed r_3 come divisore: esistono allora due interi ≥ 0 , q_4 ed r_4 , tali che $r_2=r_3*q_4+r_4$, con $r_4 < r_3$.

Si continua così, seguendo la regola: in ogni divisione che si opera il dividendo coincide con il divisore della divisione precedente, mentre il divisore coincide con il resto della divisione precedente. Queste divisioni sono possibili solo se il resto è strettamente >0 .

Questo procedimento ha sicuramente un termine, cioè esiste un resto r_n che sia nullo. Infatti se, per assurdo, tutti i resti fossero diversi da zero, l'insieme S dei resti sarebbe un insieme di numeri positivi che non avrebbe minimo (perché $r_1 < r_2 < r_3 < r_4 < \dots < r_n$) contraddicendo così l'assioma del buon ordinamento. Ci sarà allora sicuramente $r_n=0$. Supponiamo allora di avere ottenuto, ad un certo punto, un resto $r_n=0$ ed elenchiamo tutte le divisioni fatte:

$a=b*q_1+r_1$	1 ^a divisione
$b=r_1*q_2+r_2$	2 ^a divisione
$r_1=r_2*q_3+r_3$	3 ^a divisione
:	
$r_{n-4}=r_{n-3}*q_{n-2}+r_{n-2}$	terzultima divisione
$r_{n-3}=r_{n-2}*q_{n-1}+r_{n-1}$	penultima divisione
$r_{n-2}=r_{n-1}*q_n+r_n$	ultima divisione, con $r_n=0$.

Verifichiamo che l'ultimo resto non nullo r_{n-1} è il massimo comune divisore tra a e b , verifichiamo quindi che esso abbia le proprietà richieste:

1. $r_{n-1}|a$ e $r_{n-1}|b$?

dall'ultima divisione ricaviamo, essendo $r_n=0$, $r_{n-2}=r_{n-1}*q_n$, cioè che $r_{n-1}|r_{n-2}$. Dalla penultima divisione ricaviamo

$r_{n-3}=r_{n-2}*q_{n-1}+r_{n-1}=(\text{sostituendo } r_{n-2})=(r_{n-1}*q_n)*q_{n-1}+r_{n-1}=r_{n-1}*(q_n*q_{n-1}+1)$, cioè si ottiene che r_{n-1} è anche divisore di r_{n-3} . Dalla terzultima si ricava, analogamente, che r_{n-1} è anche divisore di r_{n-4} . "Risalendo" la successione di divisioni si verifica che r_{n-1} è divisore di

tutti i resti delle divisioni. Alla fine, r_{n-1} sarà divisore di r_2 ed r_1 , cioè esisteranno due interi >0 c e d tali che $r_2=r_{n-1}*c$ ed $r_1=r_{n-1}*d$. Dalla seconda divisione si ricava che $r_{n-1}|b$, essendo $b=r_1*q_2+r_2=r_{n-1}*d*q_2+r_{n-1}*c=r_{n-1}*(d*q_2+c)$;

analogamente, dalla prima divisione, si verifica che $r_{n-1}|a$.

2. se d_0 è un altro divisore comune di a e b (cioè $d_0|a$ e $d_0|b$) sarà anche vero che $d_0|r_{n-1}$?

Per dimostrarlo operiamo in maniera inversa a quanto fatto prima, cioè partiamo dalla prima divisione e “scendiamo” lungo la successione di divisioni. Per ipotesi, essendo $d_0|a$ e $d_0|b$, esisteranno due interi >0 r ed s tali che $d_0*r=a$ e $d_0*s=b$. Dalla prima divisione otteniamo:

$$r_1=a-b*q_1=d_0*r-d_0*s*q_1=d_0*(r-s*q_1) \text{ e cioè } d_0|r_1.$$

Analogamente, dalla 2^a divisione, si ricava che $d_0|r_2$ e, procedendo verso il basso lungo la successione di divisioni, che d_0 è divisore di tutti i resti. Dalla penultima divisione si ottiene che $d_0|r_{n-1}$, cioè quanto si voleva provare.

Una volta verificato che r_{n-1} gode di tutte le proprietà necessarie possiamo affermare che $r_{n-1}=m.c.d.(a,b)$.

L'algoritmo trovato permette anche di calcolare i coefficienti x e y della combinazione lineare $r_{n-1}=a*x+b*y$; infatti, dalla penultima divisione, si ricava che $r_{n-3}=r_{n-2}*q_{n-1}+r_{n-1}$ da cui: $r_{n-1}=r_{n-3}-r_{n-2}*q_{n-1}=r_{n-3}*1+r_{n-2}*(-q_{n-1})$ che dice che r_{n-1} è combinazione lineare di r_{n-3} ed r_{n-2} . Dalla terzultima divisione si ottiene: $r_{n-4}=r_{n-3}*q_{n-2}+r_{n-2}$ da cui $r_{n-2}=r_{n-4}-r_{n-3}*q_{n-2}$; sostituendo questa espressione trovata per r_{n-2} nella precedente espressione trovata per r_{n-1} otteniamo:

$r_{n-1}=r_{n-3}*1+r_{n-2}*(-q_{n-1})=r_{n-3}*1+(r_{n-4}-r_{n-3}*q_{n-2})*(-q_{n-1})=r_{n-3}*(1+q_{n-2}*q_{n-1})+r_{n-4}*(-q_{n-1})$ cioè che r_{n-1} è anche combinazione lineare di r_{n-3} ed r_{n-4} . “Risalendo” lungo la successione di divisioni si verifica che r_{n-1} è combinazione lineare di tutte le coppie di resti consecutive che lo precedono, fino ad r_1 ed r_2 . Alla fine sarà combinazione lineare di r_1 ed r_2 per cui si saranno trovati due interi t e v (che saranno in funzione dei resti e quozienti delle divisioni successive) tali che $r_{n-1}=r_1*t+r_2*v$. Arrivando alle prime due divisioni avremo:

$$a=b*q_1+r_1 \quad \text{da cui si ottiene} \quad r_1=a-b*q_1$$

$$b=r_1*q_2+r_2 \quad \text{da cui si ottiene} \quad r_2=b-r_1*q_2$$

Effettuando le sostituzioni nella combinazione lineare $r_{n-1}=r_1*t+r_2*v$ otteniamo:

$$\begin{aligned} r_{n-1} &= r_1*t+r_2*v=(a-b*q_1)*t+(b-r_1*q_2)*v=a*t+b*(-q_1*t+v)-r_1*q_1*v=a*t+b*(-q_1*t+v)-(a-b*q_1)*q_1*v= \\ &= a*(t-q_2*v)+b*(-q_2*t+v+q_1*q_2*v) \quad \text{da cui, essendo una combinazione lineare di } a \text{ e } b \\ &\text{possiamo scrivere che } x=(t-q_2*v) \text{ e } y=(-q_2*t+v+q_1*q_2*v). \end{aligned}$$

Esempio:

Trovare il m.c.d. dei numeri 231 e 60 ed i coefficienti della combinazione lineare $d=a*x+b*y$.

a	=	b	*	q ₁	+	r ₁	prima
231	=	60	*	3	+	51	divisione
b	=	r ₁	*	q ₂	+	r ₂	seconda
60	=	51	*	1	+	9	divisione
r ₁	=	r ₂	*	q ₃	+	r ₃	terza
51	=	9	*	5	+	6	divisione
r ₂	=	r ₃	*	q ₄	+	r ₄	quarta
9	=	6	*	1	+	3	divisione
r ₃	=	r ₄	*	q ₅	+	r ₅	quinta
6	=	3	*	2	+	0	divisione

Essendo $r_5=0$ il m.c.d. di a e b sarà $r_4=3$.

Troviamo i coefficienti x e y: si parte dalla penultima divisione e si torna indietro:

$$r_4=r_2-r_3=(b-r_1)-(r_1-5*r_2)=b-2*r_1+5*(b-r_1)=6*b-7*r_1=6*b-7*(a-3*b)=a*(-7)+b*27.$$

Allora $x=-7$ e $y=27$.

*Esercizio: trovare il m.c.d. tra $a=2341$ e $b=1278$ ed i coefficienti x e y della combinazione lineare $d=a*x+b*y$.*

a	=	b	*	q ₁	+	r ₁	prima
2341	=	1278	*	1	+	1063	divisione
b	=	r ₁	*	q ₂	+	r ₂	seconda
1278	=	1063	*	1	+	215	divisione
r ₁	=	r ₂	*	q ₃	+	r ₃	terza
1063	=	215	*	4	+	203	divisione
r ₂	=	r ₃	*	q ₄	+	r ₄	quarta
215	=	203	*	1	+	12	divisione
r ₃	=	r ₄	*	q ₅	+	r ₅	quinta
203	=	12	*	16	+	11	divisione
r ₄	=	r ₅	*	q ₆	+	r ₆	sesta
12	=	11	*	1	+	1	divisione
r ₅	=	r ₆	*	q ₇	+	r ₇	settima
11	=	1	*	11	+	0	divisione

Essendo $r_7=0$, $r_6=1=\text{m.c.d.}(2341,1278)$.

Troviamo i coefficienti x e y:

partiamo dalla penultima divisione ed andiamo a ritroso:

$$\begin{aligned} r_6=r_4-r_5 &= (r_2-r_3)-(r_3-16*r_4) = (b-r_1)-2*(r_1-4*r_2)+16*(r_2-r_3) = b-3*(a-b)+8*(b-r_1)+16*((b-r_1)-(r_1-4*r_2))= \\ &= -3a+4b+8b-8(a-b)+16(b-a+b-(a-b)-4(b-r_1)) = -11a+20b+16(2b-a-(a-b-4b+4(a-b)))= \\ &= -11a+20b+16(2b-a-a+5b-4a+4b) = -11a+20b+16(11b-6a) = -11a+20b+176b-96a= \\ &= a*(-107)+b*(196) \quad \text{cioè } x = -107 \text{ e } y = 196. \end{aligned}$$

Lezione n°. 14 – 20 nov. 2000

Dati due numeri interi a e b , entrambi >0 , si è definito massimo comune divisore di a e b quell'intero d che ha le proprietà:

3. $d|a$ e $d|b$;
4. d è multiplo di tutti i divisori comuni di a e b .

Si è dimostrato che il m.c.d. esiste sempre ed è della forma $d=a*x+b*y$. Non è sempre vero il viceversa: se un intero $d>0$ è combinazione lineare di due numeri interi a e b , entrambi >0 , non è detto che d sia il m.c.d.(a,b). Per esempio, possiamo scrivere $24=8*6+6*(-4)$, che dice che il numero 24 è combinazione lineare di 8 e 6, ma 24 non è il m.c.d. di 8 e 6 (non è neanche un divisore comune). Vi è, però, un caso particolare: quando $d=1$.

Teorema:

se il numero 1 è combinazione lineare degli interi a e b (entrambi >0), allora $1=m.c.d.(a,b)$.

Dimostrazione: per ipotesi $1=a*x+b*y$, con x e y numeri relativi; chiamiamo d il m.c.d. di a e b . La tesi è: $d=1$. Si avrà $d|a$ e $d|b$, quindi esisteranno due numeri interi r e t , entrambi >0 , tali che $d*r=a$ e $d*t=b$; da ciò, sostituendo nella combinazione lineare, si ottiene:

$$1=a*x+b*y=(d*r)*x+(d*t)*y=d*(r*x+t*y).$$

Quanto trovato ci dice che l'intero positivo d è divisore di 1 (essendo la quantità $(r*x+t*y)$ un numero intero) e da ciò segue che $d=1$ (1 è divisibile solo per se stesso).

Si dice che due interi positivi a e b sono **coprimi** se $m.c.d.(a,b)=1$. Per il teorema precedente, per verificare se a e b sono coprimi, basta scrivere 1 come loro combinazione lineare. Per esempio:

1. due numeri interi consecutivi sono sempre coprimi; infatti, se i due interi sono a ed $(a+1)$, allora si potrà scrivere $1=a*(-1)+(a+1)*1$ che dice che 1 è combinazione lineare di a e $(a+1)$ e quindi, per il teorema precedente, $1=m.c.d.(a, (a+1))$.
2. se a e b sono due interi positivi qualunque e se $d=m.c.d.(a,b)$, allora, essendo $d|a$ e $d|b$, esistono due numeri interi positivi r e t tali che $d*r=a$ e $d*t=b$. Si ha allora che gli interi r e t sono coprimi; infatti, d sarà combinazione lineare di a e b , cioè $d=a*x+b*y$, con x e y interi relativi, da cui, sostituendo otteniamo:

$$d=a*x+b*y=(d*r)*x+(d*t)*y=d*(r*x+t*y) \quad \text{se dividiamo entrambi i membri dell'equazione per } d \text{ otteniamo } 1=r*x+t*y, \text{ che è una combinazione lineare degli interi } r$$

e t che da come risultato 1 e quindi, per il teorema precedente, $1 = \text{m.c.d.}(r, t)$ per cui gli interi r e t sono coprimi.

Se un numero intero positivo a è divisore di un prodotto di due interi b e c , entrambi >0 , cioè $a|(b*c)$ non è detto che a sia divisore di almeno uno dei due interi b e c ; per esempio, $8|(6*4)$ eppure $8 \nmid 6$ e $8 \nmid 4$.

Vi è, però, un caso particolare: se l'intero a è un numero primo.

Teorema:

se un numero intero primo $a > 0$ è divisore di un prodotto di due numeri interi positivi b e c , allora a è divisore di almeno uno dei fattori b o c (o entrambi).

Dimostrazione: per ipotesi $a|(b*c)$, cioè esiste un numero intero $z > 0$ tale che $a*z = b*c$. Per ottenere la tesi basta verificare che, se a non è divisore di uno dei due fattori, a sarà divisore dell'altro. Supponiamo allora che $a \nmid b$ e verifichiamo che $a|c$; calcoliamo il $\text{m.c.d.}(a, b)$: se chiamiamo d tale $\text{m.c.d.}(a, b)$, si ha che d è un divisore comune di a e b , ma a è un numero primo ed ammette solo i divisori banali, quindi può essere solamente $d=1$ oppure $d=a$. Ma deve essere $d \neq a$ (perché $d|b$ e stiamo supponendo che a non lo è), per cui si conclude che $d=1$. Tale $\text{m.c.d.}(a, b)$ si può scrivere come combinazione lineare di a e b , cioè $d=1=a*x+b*y$, con x e y interi relativi. Se moltiplichiamo entrambi i membri dell'equazione per c otteniamo:

$c = a*c*x + b*c*y$ ricordando che, essendo $a|(b*c)$, è $b*c = a*z$, si ha, sostituendo,
 $c = a*c*x + a*z*y = a*(c*x + z*y)$. Poiché la quantità $(c*x + z*y)$ è un intero positivo possiamo dedurre che $a|c$.

Osservazione: il teorema precedentemente dimostrato vale anche per prodotti di più di due fattori (per 3, per 4 etc.). Per esempio, se i fattori sono 3: se il numero primo $a > 0$ è divisore del prodotto di 3 numeri interi b, c, e , tutti >0 , allora a è divisore di almeno uno dei tre interi b , c oppure e . Infatti, $a|(b*c*e)$, cioè $a|((b*c)*e)$ ed in questo modo è come se avessimo due fattori $((b*c)$ ed e) e, per il teorema precedente a è divisore di $(b*c)$ oppure a è divisore di e . Applicando nuovamente il teorema per $(b*c)$ alla fine otteniamo che a sarà divisore di almeno uno tra i numeri interi b , c ed e .

Teorema di fattorizzazione unica.

Ogni intero $a > 1$ si può rappresentare come prodotto di numeri interi primi. (la parola *prodotto* indica, al limite, anche il prodotto di un solo fattore; senza questa puntualizzazione non potremmo rappresentare i numeri primi, visto che il numero 1 non è

primo). Inoltre, tale fattorizzazione è unica (a meno dell'ordine dei fattori, nel senso che, se sono date due fattorizzazioni in prodotti di numeri primi per lo stesso intero $a > 1$:

$a = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$, con $p_1 \dots p_r$ e $q_1 \dots q_s$ numeri primi, allora il numero di fattori è uguale nelle due fattorizzazioni, cioè $r = s$, e, riordinando opportunamente i fattori, essi sono gli stessi, cioè $p_1 = q_1, p_2 = q_2, \dots, p_r = q_s$).

Dimostrazione:

1. esistenza della fattorizzazione: preso un intero $a > 1$ qualunque, la tesi è che a si può rappresentare come prodotto di numeri primi. Per assurdo, supponiamo che esista qualche intero > 1 che non sia prodotto di numeri primi: raccogliamo allora in un insieme S tali interi: $S = \{ x / x \text{ è un intero } > 1 \text{ e } x \text{ non è prodotto di numeri primi} \}$. Per l'assioma del buon ordinamento, esiste in S un numero minimo $s \in S$ (cioè s è un numero intero > 1 ed s non è prodotto di numeri primi). Osserviamo che s non è un numero primo (perché se lo fosse sarebbe prodotto di numeri primi con un solo fattore); allora s ha un divisore z non banale: $z | s$ con $1 < z < s$. Essendo $z | s$ esisterà un numero intero $t > 0$ tale che $z \cdot t = s$, ma anche t è un divisore non banale di s (perché certamente $t \neq 1$ e $t \neq s$, essendo $z \neq 1$ e $z \neq s$) e quindi $1 < t < s$. Essendo s il numero minimo dell'insieme S , allora t e z non appartengono ad S . Allora z e t sono prodotti di numeri primi, il che implica che $s = z \cdot t$ è, a sua volta un prodotto di numeri primi, contraddicendo l'ipotesi fatta per assurdo. Allora possiamo dire che la fattorizzazione in prodotto di numeri primi per un numero intero $a > 1$ esiste sempre.

Lezione n°. 15 – 22 nov. 2000

Dimostrazione dell'unicità della fattorizzazione: sia $a = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$ (con $p_1 \dots p_r$ e $q_1 \dots q_s$ numeri primi). Si nota che $(p_1) \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$, ossia che p_1 è divisore del prodotto $(q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s)$ e quindi, per una proprietà dei numeri primi già dimostrata, p_1 è divisore di almeno uno dei fattori $q_1, q_2, q_3, \dots, q_s$. Riordinando opportunamente, in modo da portare al posto q_1 il fattore di cui p_1 è divisore, si ottiene che $p_1 | q_1$. Ma q_1 è un numero primo ed ha come divisori quelli banali, cioè 1 e q_1 , ma il numero 1 non è primo, quindi deve essere $p_1 \neq 1$ ed allora $p_1 = q_1$. Dividendo l'eguaglianza per p_1 si ottiene allora:

$$p_2 \cdot p_3 \cdot \dots \cdot p_r = q_2 \cdot q_3 \cdot \dots \cdot q_s.$$

Con lo stesso ragionamento possiamo scrivere :

$$(p_2) \cdot p_3 \cdot \dots \cdot p_r = q_2 \cdot q_3 \cdot \dots \cdot q_s \Rightarrow p_2 | (q_2 \cdot q_3 \cdot \dots \cdot q_s) \Rightarrow p_2 \text{ è divisore di almeno uno dei fattori } q_2, q_3, \dots, q_s \text{ ed allora, riordinando opportunamente possiamo ottenere } p_2 | q_2 \text{ e,}$$

visto che q_2 è numero primo e $p_2 \neq 1 \Rightarrow p_2 = q_2$. Dividendo entrambi i membri dell'eguaglianza per p_2 si ottiene $p_3 \cdot p_4 \cdot \dots \cdot p_r = q_3 \cdot q_4 \cdot \dots \cdot q_s$. Ripetendo per ogni p_i lo stesso procedimento si ottiene che $p_1 = q_2$, $p_2 = q_2$, etc., come si voleva dimostrare. Rimane da dimostrare che $r = s$. Se, per assurdo, fosse $r \neq s$, per esempio se fosse $r < s$, dopo r applicazioni del procedimento precedente si otterrebbe:

$1 = q_{r+1} \cdot q_{r+2} \cdot \dots \cdot q_s$ e ciò è una contraddizione in quanto ogni numero primo $q_{r+1} \dots q_s$ (per la definizione stessa di numero primo) è > 1 ed il prodotto di numeri > 1 sarà sempre > 1 e quindi non può mai essere $= 1$ come trovato, quindi $r = s$ ed il teorema di fattorizzazione unica è dimostrato anche per quanto riguarda l'unicità.

Conseguenze del teorema di fattorizzazione unica.

1. vi sono infiniti numeri primi (Euclide), infatti se, per assurdo, tutti i numeri primi fossero un numero finito, li potremmo elencare in un insieme: $\{p_1, p_2, \dots, p_m\}$. Consideriamo il seguente numero intero $a > 1$, $a = (p_1 \cdot p_2 \cdot \dots \cdot p_m) + 1$. Per il teorema di fattorizzazione unica tale a ha un prodotto di numeri primi (scelti, ovviamente nell'insieme $\{p_1, p_2, \dots, p_m\}$, che abbiamo supposto racchiudere *tutti* i numeri primi). Fissiamo, a piacere, un fattore primo di a e sia esso p_i (con i compreso tra 1 ed m): allora $p_i | a$, cioè esisterà in intero $c > 0$ tale che $a = p_i \cdot c$ per cui possiamo scrivere:

$$a = (p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_m) + 1 \quad \text{da cui}$$

$$1 = a - (p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_m) = (p_i \cdot c) - (p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_m) = p_i \cdot (c - (p_1 \cdot p_2 \cdot \dots \cdot p_m))$$

L'eguaglianza trovata è però contraddittoria perché avremmo trovato un divisore p_i per il numero 1, che ammette come divisore solo se stesso ed essendo $p_i > 1$ (in quanto numero primo) non può essere $p_i = 1$. Possiamo quindi affermare che i numeri primi sono infiniti.

2. $\sqrt{2}$ è un numero irrazionale; per assurdo, se fosse $\sqrt{2}$ razionale, si potrebbe scrivere: $\sqrt{2} = a/b$, con a e b numeri interi. Elevando al quadrato otterremo $2 = a^2/b^2$ da cui $2b^2 = a^2$.

Si possono avere 4 casi:

- a) $a = b = 1$;
- b) $a > 1$ e $b = 1$;
- c) $a = 1$ e $b > 1$;
- d) $a > 1$ e $b > 1$.

Si intuisce facilmente che, per i casi a, b e c si arriva ad una contraddizione; nel caso d, per il teorema di fattorizzazione unica, sia a che b sono prodotti di numeri primi:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r$$

$b = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s$ sostituendo nella uguaglianza $2b^2 = a^2$ otteniamo:

$$2 \cdot (q_1^2 \cdot q_2^2 \cdot q_3^2 \cdot \dots \cdot q_s^2) = p_1^2 \cdot p_2^2 \cdot p_3^2 \cdot \dots \cdot p_r^2$$

Osservando che, nella fattorizzazione di un quadrato, i numeri primi compaiono un numero pari di volte (perché raddoppiano rispetto al numero di volte che compaiono nella base del quadrato), troviamo una contraddizione nell'uguaglianza precedente, perché il numero 2 comparirà un numero pari di volte al secondo membro ed un numero dispari di volte al primo membro e ciò non è possibile perché si avrebbero due fattorizzazioni diverse (di uguale valore) e si andrebbe contro il teorema di fattorizzazione unica.

Lezione n°. 16 – 24 nov. 2000

Relazioni tra insiemi.

Se A e B sono due insiemi, si dice relazione da A a B una qualunque regola che faccia corrispondere elementi di A con elementi di B (possono esistere elementi di A che non corrispondono ad elementi di B o che corrispondono a più di un elemento di B).

Una relazione si indica con una lettera maiuscola (in genere R, S...) e, per esprimere simbolicamente che l'elemento $a \in A$ corrisponde all'elemento $b \in B$, si scrive aRb (*a è in relazione con b*). Se, invece, $a \in A$ **non è** in corrispondenza con $b \in B$ si scrive $a \nR b$.

Vi sono due modi di esprimere una relazione R da A a B:

- a) modo esplicito: si elencano tutte le coppie formate da un elemento di A ed un elemento di B associati tra loro (questo modo però si può utilizzare solo con insiemi finiti).

Esempio: $A = \{1, 2, 4, 7\}$, $B = \{2, 3, 5, 8\}$. Una relazione da A a B può essere la seguente:

1R2, 1R3, 1R5, 1R8, 2R3, 2R5, 2R8, 4R5, 4R8, 7R8.

- b) modo implicito: si usa un predicato in due variabili $P(x, y)$, dove la prima variabile ha come campo di variabilità l'insieme A e la seconda ha come campo di variabilità l'insieme B. Con tale predicato si fa corrispondere un elemento $a \in A$ con un elemento $b \in B$ quando la proposizione $P(a, b)$ che si ottiene sostituendo la coppia (a, b) alla coppia (x, y) è vera. Riferendoci all'esempio precedente la relazione si può descrivere implicitamente con il predicato $P(x, y) = "x < y"$. Non sempre è possibile estrapolare un predicato sintetico ed immediato per descrivere in modo implicito la relazione.

Relazioni binarie.

Se $A = B$, una relazione da A ad A viene detta relazione binaria definita in A.

Relazioni di equivalenza.

Sia R una relazione binaria definita nell'insieme A .

Si dice che R soddisfa la *proprietà riflessiva* se ogni elemento di A è in corrispondenza con se stesso (oltre che, eventualmente, con altri), simbolicamente: $\forall a \in A \Rightarrow aRa$.

Si dice che R soddisfa la *proprietà simmetrica* se, ogni volta che un elemento $a \in A$ è in corrispondenza con un elemento $b \in A$, anche b è in corrispondenza con a ; in simboli:

$$\forall a, b \in A, aRb \Rightarrow bRa.$$

Si dice che R soddisfa la *proprietà transitiva* se, ogni volta che un elemento $a \in A$ è in corrispondenza con un elemento $b \in A$, e $b \in A$ è in corrispondenza con $c \in A$ allora anche a è in corrispondenza con c ; in simboli: $\forall a, b, c \in A, aRb \text{ e } bRc \Rightarrow aRc$.

Una relazione binaria definita nell'insieme A , se soddisfa le tre proprietà riflessiva, simmetrica e transitiva è detta *relazione di equivalenza*.

Esempio 1:

Sia $A = \mathbb{Z}$ (insieme dei numeri relativi) e definiamo una relazione binaria in \mathbb{Z} implicitamente con il predicato $P(x, y) = "x * y > 0"$.

Vediamo se questa è un relazione di equivalenza, verificando se soddisfa le tre proprietà:

- proprietà simmetrica: se $a, b \in \mathbb{Z}$ e se aRb è vero che bRa ?
Se aRb vuol dire che $a * b > 0$ da cui, certamente $b * a > 0$ (perché $a * b = b * a$) e quindi bRa .
- Proprietà transitiva: $a, b, c \in \mathbb{Z}$ e se aRb e bRc è vero che aRc ?
Se aRb e bRc si ha che $a * b > 0$ e $b * c > 0$, quindi a e b sono $\neq 0$ ed hanno lo stesso segno; analogamente b e c sono $\neq 0$ ed hanno lo stesso segno; allora a e c sono $\neq 0$ ed hanno lo stesso segno di b , cioè a e c hanno lo stesso segno per cui $a * c > 0$ cioè aRc .
- Proprietà riflessiva: è vero che $\forall a \in \mathbb{Z} \Rightarrow aRa$? Non è vero perché c'è il caso di $a=0$ in cui $a * a$ non è strettamente maggiore di 0.

Allora la relazione R non è una relazione di equivalenza.

Esercizio: se la relazione precedente è modificata con la seguente $P(x, y) = "x * y \geq 0"$, valgono le tre proprietà?

Svolgimento:

- Proprietà riflessiva: è vero che $\forall a \in \mathbb{Z} \Rightarrow aRa$? Sì, perché con la nuova relazione si comprende anche il caso di $a=0$ (se $a \neq 0$ $a * a > 0$ sempre, se $a=0$ si ha il caso $a * a = 0$).

- proprietà simmetrica: se $a, b \in \mathbb{Z}$ e se aRb è vero che bRa ?
Se aRb vuol dire che $a*b \geq 0$ da cui, certamente $b*a \geq 0$ (perché $a*b = b*a$) e quindi bRa .
- Proprietà transitiva: $a, b, c \in \mathbb{Z}$ e se aRb e bRc è vero che aRc ?
Se aRb e bRc si ha che $a*b \geq 0$ e $b*c \geq 0$; possiamo avere diversi casi;
 - a e b sono $\neq 0$ e quindi hanno lo stesso segno; se $c=0$ $a*c=0$ quindi vale aRc , se $c \neq 0$ avrà lo stesso segno di b (e quindi lo stesso di a per cui vale aRc);
 - $a=0$ e $b \neq 0$; in questo caso, qualunque sia il segno di c aRc vale (perché $a*c=0$);
 - $a \neq 0$ e $b=0$; se $c=0$ allora $a*c=0$ e vale aRc , se $c \neq 0$ aRc vale solo nel caso in cui a e c hanno lo stesso segno, per cui, la proprietà transitiva non è verificata per ogni elemento di \mathbb{Z} .

In conclusione la relazione R non è una relazione di equivalenza.

Esempio 2:

Sia $A = \mathbb{Z}$; definiamo una relazione R in \mathbb{Z} con il predicato

$P(x, y) = \text{"esiste un numero relativo } z \in \mathbb{Z} \text{ tale che } x - y = 3*z"$.

(Es.: $3R(-6)$ perché $\exists z=3 / 3 - (-6) = 9 = 3*3$; $5 \nR 7$ perché non esiste $z \in \mathbb{Z}$ tale che $3*z = 5 - 7 = 2$)

Tale relazione è di equivalenza?

Verifichiamo se soddisfa le tre proprietà:

- Riflessiva: ogni elemento $a \in \mathbb{Z}$ è in corrispondenza con se stesso, cioè aRa ? Poiché $a - a = 0$, $\exists z=0$ tale che $a - a = 0 = 3*0$ per cui la proprietà riflessiva è soddisfatta.
- Simmetrica: dati $a, b \in \mathbb{Z}$ se aRb è vero che bRa ? Se aRb significa che $\exists z \in \mathbb{Z}$ tale che $a - b = 3*z$. bRa significa $b - a = -(a - b) = -3*z = 3*(-z)$, quindi esiste in \mathbb{Z} l'opposto di z che rende vero bRa , per cui anche la proprietà simmetrica è soddisfatta;
- Transitiva: dati $a, b, c \in \mathbb{Z}$ se aRb e bRc è vero che aRc ? Se $aRb \exists z \in \mathbb{Z}$ tale che $a - b = 3*z$, e se $bRc \exists v \in \mathbb{Z}$ tale che $b - c = 3*v$; se sommiamo membro a membro le due espressioni otteniamo $a - b + (b - c) = 3*z + 3*v$ cioè $a - c = 3*(z+v)$; essendo $(z+v)$ un intero relativo possiamo affermare che $\exists (z+v) \in \mathbb{Z}$ tale aRc , per cui anche la proprietà transitiva è soddisfatta.

In conclusione, essendo soddisfatte tutte e tre le proprietà, la relazione R è una relazione di equivalenza in \mathbb{Z} .

Lezione n°. 17 – 27 nov. 2000

Se A e B sono due insiemi finiti, una relazione da A a B si può rappresentare in altri due modi: **forma matriciale** e **forma grafica**.

Rappresentazione matriciale.

Siano $A=\{a_1, a_2, \dots, a_n\}$ e $B=\{b_1, b_2, \dots, b_m\}$ e sia data la relazione R da A a B. La rappresentazione matriciale di R si ottiene costruendo una tabella (detta *matrice*) che ha n righe (corrispondenti agli elementi di A) ed m colonne (corrispondenti agli elementi di B).

	b_1	b_2	b_3	b_4	b_m
a_1								
a_2								
a_3								
..								
..								
a_n								

Ogni casella della matrice viene riempita con un valore che può essere 0 oppure 1 secondo il criterio: all'incrocio tra la riga corrispondente ad un elemento di A ed una colonna corrispondente ad un elemento di B si inserisce il valore 1 se i due elementi sono associati nella relazione R, si inserisce il valore 0 se nel caso contrario.

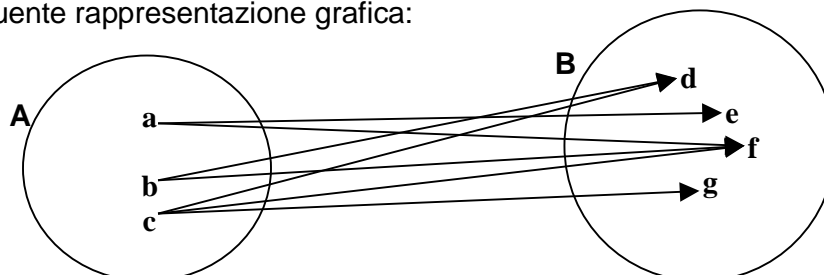
Esempio:

Se $A=\{a,b,c\}$ e $B=\{d,e,f,g\}$ allora la seguente matrice è la rappresentazione matriciale della relazione descritta esplicitamente da aRe , aRf , bRd , bRf , cRd , cRf , cRg .

	d	e	f	g
a	0	1	1	0
b	1	0	1	0
c	1	0	1	1

Rappresentazione grafica.

Si usano i diagrammi di Eulero-Venn, quindi si avrà un diagramma per l'insieme A ed uno per l'insieme B. Si disegnano delle frecce che partono dagli elementi di A ed arrivano agli elementi di B ad essi associati dalla relazione R. In riferimento all'esempio precedente si avrà la seguente rappresentazione grafica:



Esercizio: Se A è un insieme finito e se R è una relazione da A in A , nella sua rappresentazione matriciale quale proprietà ha la matrice quando vale proprietà riflessiva? E quale proprietà ha la matrice quando vale la proprietà simmetrica?

Svolgimento: nel caso della proprietà riflessiva avremo una matrice quadrata con le caselle della diagonale che va dal vertice in alto a sinistra al vertice in basso a destra piene solo di 1, infatti la proprietà riflessiva dice che aRa , bRb , cRc etc.

Nel caso della proprietà simmetrica si avrà una matrice quadrata con le caselle che si trovano in posizione simmetrica rispetto alla diagonale che va dal vertice in alto a sinistra al vertice in basso a destra piene dello stesso valore, infatti la proprietà simmetrica dice che se aRb sarà anche bRa , se aRc sarà anche cRa etc.

	a	b	c
a	1	1	1
b	1	1	1
c	0	0	1

Se vale la proprietà riflessiva.

	a	b	c
a	1	1	1
b	1	1	0
c	1	0	0

Se vale la proprietà simmetrica.

Classe di equivalenza.

Siano A un insieme ed R una relazione di equivalenza definita in A e fissiamo un elemento $a \in A$. Si definisce *classe di equivalenza rappresentata da a* il sottoinsieme di A (indicato con $[a]$) che contiene esattamente tutti gli elementi di A che sono associati all'elemento a .
 $[a] = \{x \in A / xRa\}$ (notare che scrivere aRx o xRa è la stessa cosa perché, essendo R una relazione di equivalenza, vale la proprietà simmetrica oltre, naturalmente, le proprietà riflessiva e transitiva.)

La classe $[a]$ è certamente un sottoinsieme non vuoto perché contiene almeno l'elemento a (per la proprietà riflessiva).

Esempio:

Sia $A = \mathbb{N}$ e definiamo la relazione in A con il predicato $P(x,y) = "x+y \text{ è pari}"$.

Essa è una relazione di equivalenza, infatti valgono le tre proprietà:

- riflessiva: $\forall a \in \mathbb{N} \ a+a=2$ e qualsiasi numero moltiplicato per 2 è pari.
- Simmetrica: vale la proprietà commutativa della somma per cui $x+y=y+x$.
- Transitiva: se aRb si ha che $a+b$ è pari e se bRc si ha che $b+c$ è pari. Sommando due numeri pari otteniamo ancora un numero pari, quindi $(a+b)+(b+c)$ è pari. Ma $(a+b)+(b+c)=a+2b+c$ ed essendo $2b$ pari, se sottraiamo ad un numero pari una quantità pari otterremo ancora un numero pari e cioè $(a+2b+c)-2b=a+c$ è pari.

Prendiamo un esempio di classe di equivalenza: fissiamo, per esempio, $a=3 \in \mathbb{N}$.

$[3] = \{x \in \mathbb{N} / xR3 \text{ cioè } x+3 \text{ è pari}\} = \{\text{tutti i numeri naturali dispari}\}$.

Se prendiamo un altro elemento può capitare di avere un'altra classe di equivalenza identica all'altra:

$[7] = \{x \in \mathbb{N} / xR7 \text{ cioè } x+7 \text{ è pari}\} = \{\text{tutti i numeri naturali dispari}\}$.

Pur essendo i rappresentanti $a=3$ ed $a=7$ diversi tra loro, la classe può risultare la stessa: le due classi si chiamano *classe 3* e *classe 7*.

Se consideriamo la classe di equivalenza:

$[4] = \{x \in \mathbb{N} / xR4 \text{ cioè } x+4 \text{ è pari}\} = \{\text{tutti i numeri naturali pari}\}$.

Con il predicato $P(x,y) = "x+y \text{ è pari}"$ si possono ottenere solo due classi di equivalenza, cioè i numeri naturali dispari ed i numeri naturali pari, perché, per quanto si cambino i rappresentanti, le classi non variano.

Esercizio:

Sia A l'insieme dei numeri relativi non nulli, $A = \mathbb{Z} - \{0\}$, e si definisca in A la relazione R mediante il predicato $P(x,y) = "x*y > 0"$. Dimostrare che R è una relazione di equivalenza e trovare tutte le classi di equivalenza. (il problema è: quale è il criterio con cui, data una relazione di equivalenza R in A si può stabilire se la classe $[a]$ è uguale alla classe $[b]$?).

Svolgimento:

- Proprietà riflessiva: aRa significa $a*a$ ed essendo $a \neq 0$ (perché A è l'insieme dei numeri relativi non nulli) $a*a$ è sempre >0 in quanto è un quadrato;
- proprietà simmetrica: se $a,b \in A$ e se aRb è vero che bRa ?

Se aRb vuol dire che $a*b > 0$ da cui, certamente $b*a > 0$ (perché $a*b = b*a$) e quindi bRa .

- Proprietà transitiva: $a, b, c \in A$ e se aRb e bRc è vero che aRc ?

Se aRb e bRc si ha che $a \cdot b > 0$ e $b \cdot c > 0$, quindi a e b hanno lo stesso segno; analogamente b e c hanno lo stesso segno; allora a e c hanno lo stesso segno di b , cioè a e c ha lo stesso segno per cui $a \cdot c > 0$ cioè aRc .

La relazione R è allora una relazione di equivalenza in A .

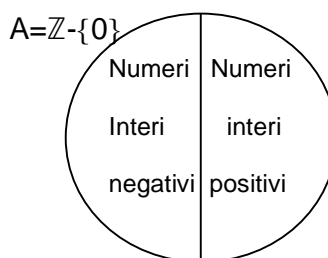
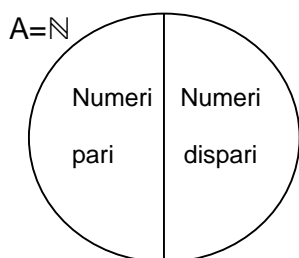
Le classi di equivalenza possibili sono 2:

$[1] = \{x \in A / xR1 \text{ cioè } x \cdot 1 > 0\} = \{\text{tutti i numeri positivi}\}$.

$[-1] = \{x \in A / xR(-1) \text{ cioè } x \cdot (-1) > 0\} = \{\text{tutti i numeri negativi}\}$.

Lezione n°. 18 – 29 nov. 2000

Nei due esempi di relazioni di equivalenza visti in precedenza si sono trovate due classi di equivalenza (pari e dispari) nell'insieme \mathbb{N} e due classi di equivalenza (positivi e negativi) in $A = \mathbb{Z} - \{0\}$. Se si rappresentano le classi graficamente, si nota che, in entrambi i casi, le due classi trovate non hanno elementi comuni (cioè la loro intersezione è vuota) e che la loro unione dà tutto l'insieme di partenza. Questo avviene per ogni relazione di equivalenza. (Nota: non sempre, invece le classi di equivalenza sono due ma possono anche essere di più).



Esiste il seguente

Teorema: siano A un insieme ed R una relazione di equivalenza definita in A ; allora:

1. due classi equivalenza diverse hanno intersezione vuota, cioè non hanno elementi in comune;
2. l'unione di tutte le classi di equivalenza dà tutto l'insieme A .

Prima di procedere alla dimostrazione del teorema premettiamo un lemma:

lemma: siano A un insieme ed R una relazione di equivalenza definita in A ; allora, dati due elementi a e $b \in A$ si ha che $[a] = [b] \Leftrightarrow aRb$.

(questo lemma dà un criterio per verificare se due elementi rappresentano la stessa classe di equivalenza).

Dimostrazione del lemma: supponiamo (1^a ipotesi) che $[a]=[b]$ e verifichiamo (tesi) che aRb . Per la proprietà riflessiva di R aRa quindi $a \in [a]$ per cui, essendo per ipotesi $[a]=[b]$ si ha che $a \in [b]$, cioè aRb , come volevasi dimostrare.

Viceversa, supponiamo (2^a ipotesi) che aRb e verifichiamo che $[a]=[b]$ (tesi). Essendo $[a]$ e $[b]$ due insiemi la tesi corrisponde ad una “doppia inclusione”, cioè $[a] \subseteq [b]$ e $[a] \supseteq [b]$; dimostriamo la prima inclusione (la seconda si dimostra in maniera analoga): prendiamo un qualunque elemento $x \in [a]$ e verifichiamo se $x \in [b]$. Se $x \in [a]$ si ha xRa e, visto che per ipotesi aRb , per la proprietà transitiva della relazione di equivalenza R , si avrà xRb , cioè $x \in [b]$, come volevasi dimostrare.

Lezione n°. 19 – 1 dic. 2000

Dimostrazione del teorema:

siano A un insieme ed R una relazione di equivalenza definita in A ; allora:

1. due classi di equivalenza diverse hanno intersezione vuota, cioè non hanno elementi in comune;
2. l'unione di tutte le classi di equivalenza dà tutto l'insieme A .

Dimostrazione parte 1: Siano $[a]$ e $[b]$ due classi di equivalenza diverse in A e dimostriamo che $[a] \cap [b] = \emptyset$. Per assurdo, se ciò non fosse vero ($[a] \cap [b] \neq \emptyset$), esisterebbe un elemento $c \in [a] \cap [b]$; ma ciò significa che $c \in [a]$ e $c \in [b]$ e, da $c \in [a]$, seguirebbe cRa mentre da $c \in [b]$ seguirebbe cRb : allora, per la proprietà simmetrica di R , da cRa seguirebbe aRc e, per la proprietà transitiva di R da aRc e cRb seguirebbe aRb e, per il lemma prima dimostrato, $aRb \Leftrightarrow [a]=[b]$, cioè se fosse $[a] \cap [b] \neq \emptyset$, si andrebbe in contraddizione con l'ipotesi del teorema (le due classi sono diverse).

Dimostrazione parte 2: per dimostrare questa parte del teorema basta dimostrare che ogni elemento $a \in A$ è contenuto in almeno una classe e, in effetti ciò è vero perché, per la proprietà riflessiva di R , ogni elemento $a \in [a]$.

Congruenze.

Sia \mathbb{Z} l'insieme di tutti i numeri relativi: fissato un numero intero $m > 1$ (detto **modulo**) si definisce una relazione di equivalenza in \mathbb{Z} , detta **congruenza modulo m** , tramite il predicato: $P(x,y) = \text{“esiste un numero intero } k \in \mathbb{Z} \text{ tale che } (x-y) = m \cdot k\text{”}$.

(tale relazione è già stata costruita in precedenza come esempio per il caso $m=3$ —pag.40).

Dimostriamo che R è una relazione di equivalenza:

Proprietà riflessiva: è verificata perché $\forall a \in \mathbb{Z}$ esiste $k=0$ tale che $a-a=0=m*0$, cioè aRa ;

proprietà simmetrica: è verificata perché $\forall a,b \in \mathbb{Z}$, se aRb (cioè $\exists k \in \mathbb{Z} / a-b=m*k$) negando

entrambi i membri si ottiene $-(a-b)=b-a= -m*k=m*(-k)$ cioè $\exists (-k) \in \mathbb{Z} / b-a=m*(-k)$, cioè bRa ;

proprietà transitiva: è verificata perché $\forall a,b,c \in \mathbb{Z}$, se aRb e bRc significa che esistono due interi $k,h \in \mathbb{Z}$ tali che:

$$a-b=m*k$$

$b-c=m*h$ da cui, sommando membro a membro si ottiene: $(a-b)+(b-c)=a-c=m*(k+h)$ e, essendo la somma $(k+h)$ di due numeri interi ancora un numero intero, si ha che

$$\exists (k+h) \in \mathbb{Z} / a-c=m*(-k), \text{ cioè } aRc.$$

La relazione R è allora una relazione di equivalenza in \mathbb{Z} .

La relazione così definita dipende dal modulo e, quindi, ci sarà la congruenza modulo 2, la congruenza modulo 3 etc. Per distinguere ognuna di tali relazioni si utilizza una simbologia particolare: invece di aRb si scrive **$a \equiv b \pmod{m}$** che si legge *a congruo b modulo m*.

Il simbolo $\not\equiv$ si userà quando non vale la congruenza.

Esempi:

$$3 \equiv (-7) \pmod{5} \text{ perché } 3-(-7)=10=5*2.$$

$$4 \not\equiv (-11) \pmod{2} \text{ perché } 4-(-11)=15 \text{ non si può scrivere nella forma } 2*k, \text{ con } k \in \mathbb{Z}.$$

Nello studio delle classi di congruenza sorgono le seguenti domande:

1. come sono fatti gli elementi di una classe di congruenza?
2. quanti sono gli elementi di una classe di congruenza?
3. quante sono le classi di congruenza?

Cerchiamo di rispondere:

1. fissato $a \in \mathbb{Z}$ la classe rappresentata da a è:

$$[a]=\{x \in \mathbb{Z} / x \equiv a \pmod{m}\}=\{x \in \mathbb{Z} / x-a=m*k, \text{ con } k \in \mathbb{Z}\}=\{x / x=a+m*k, \text{ con } k \in \mathbb{Z}\}$$

Poiché a ed m sono fissati, facendo variare k si ottengono tutti gli elementi di una classe di congruenza, quindi: $[a]=\{a, (a+m), (a-m), (a+2m), (a-2m), \dots \text{etc.}\}$

2. dalla individuazione del *come* sono fatti gli elementi di $[a]$ si ottiene anche la risposta alla seconda domanda, essi sono cioè infiniti.

Esempio: consideriamo la classe di congruenza modulo 4:

$$[1] = \{x \in \mathbb{Z} / x=1+4k, \text{ con } k \in \mathbb{Z}\} = \{1, 5, -3, 9, \dots\}.$$

Per costruire un'altra classe di congruenza risulta inutile prendere una classe $[a]$ con $a \equiv 1 \pmod{4}$ perché, per il lemma precedentemente dimostrato, $aR1 \Rightarrow [a]=[1]$.

Consideriamo allora un elemento $a \notin [1]$, ad esempio $a=2$ ($2 \not\equiv 1 \pmod{4}$ perché $2-1=1$ non si può scrivere nella forma $4 \cdot k$). Allora $[2] \neq [1]$, ed inoltre, per il teorema, sappiamo anche che si otterrà un insieme tale che $[2] \cap [1] = \emptyset$:

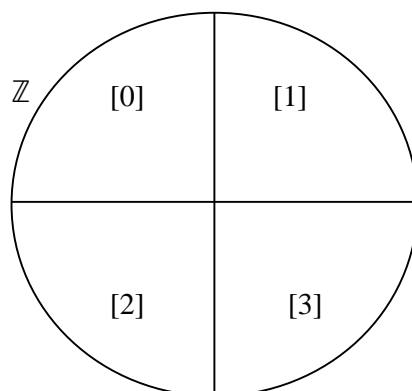
$$[2] = \{x \in \mathbb{Z} / x=2+4k, \text{ con } k \in \mathbb{Z}\} = \{2, 6, 10, -2, \dots\}$$

Prendendo, per esempio $a=0$ notiamo che $0 \not\equiv 1 \pmod{4}$ e $0 \not\equiv 2 \pmod{4}$ quindi $[0] \neq [1]$ e

$$[0] \neq [2]: [0] = \{x \in \mathbb{Z} / x=0+4k, \text{ con } k \in \mathbb{Z}\} = \{0, 4, -4, 8, -8, \dots\}.$$

Esiste anche $[3] = \{x \in \mathbb{Z} / x=3+4k, \text{ con } k \in \mathbb{Z}\} = \{3, 7, 11, -1, \dots\}$.

Graficamente ogni classe di congruenza rappresenta una “fetta” dell'insieme di partenza \mathbb{Z} :



Il problema da risolvere per dare risposta alla terza domanda è: esiste un intero $a \in \mathbb{Z}$ tale che $a \not\equiv 1 \pmod{4}$, $a \not\equiv 2 \pmod{4}$, $a \not\equiv 3 \pmod{4}$ e $a \not\equiv 0 \pmod{4}$? Cioè esistono altre classi di congruenza modulo 4? La risposta viene fornita da un teorema (che sarà dimostrato in seguito) che dice: le classi di congruenza modulo m sono in numero di m .

Lezione n°. 20 – 4 dic. 2000

Le classi di congruenza sono della forma $[a]=\{x \in \mathbb{Z} / x=a+m*k \text{ con } k \in \mathbb{Z}\}$.

Dimostreremo che le classi di congruenza modulo m sono in numero di m , dimostrando il seguente teorema:

teorema:

- a) le classi di congruenza modulo m sono tutte e sole le seguenti: $[0],[1],[2],\dots,[m-2],[m-1]$.
- b) Tutte le classi sopra elencate sono diverse tra loro (e quindi sono in numero di m).

Dimostrazione:

a) Presa una qualunque classe di congruenza $[a]$, si deve dimostrare che essa coincide con una delle classi $[0],[1],[2],\dots,[m-1]$. Nel caso in cui $a \geq 0$, utilizzando l'algoritmo della divisione prendendo a come dividendo ed m come divisore, si avrà che esistono un quoziente ed un resto (numeri interi) $q, r \geq 0$ tali che $a=m*q+r$, con $r < m$. Da ciò notiamo che $a-r=m*q$, cioè $a \equiv r \pmod{m}$. Ricordando il lemma che dice che $[a]=[b] \Leftrightarrow aRb$, si ottiene che $[a]=[r]$. Poiché è $r < m$ ed $r \geq 0$, segue che r può assumere solamente valori compresi fra 0 ed $m-1$ con la conseguenza che $[a]$ coincide allora veramente con una delle classi $[0],[1],[2],\dots,[m-1]$. Si è quindi dimostrato la prima parte del teorema, ma solo per il caso $a \geq 0$. Nel caso $a < 0$ consideriamo il numero opposto di a , cioè $(-a) > 0$ ed utilizziamo ancora l'algoritmo della divisione dividendo $(-a)$ per m : otterremo un quoziente ed un resto (numeri interi) $q, r \geq 0$ tali che $(-a)=m*q+r$, con $r < m$. Si dovranno distinguere adesso i due casi possibili:

1. $r=0$: in questo caso si avrebbe $(-a)=m*q$ cioè $a=-m*q=m*(-q)$ quindi $a=0=m*(-q)$ che dice che $a \equiv 0 \pmod{m}$ e, sempre per il lemma usato prima, $[a]=[0]$, cioè è valido il postulato del teorema.
2. $r>0$: in questo caso consideriamo il numero $(m-r)$, che sarà uno dei numeri compresi tra 1 ed $(m-1)$, perché i valori possibili di r sono $1,2,\dots,m-1$ e quindi i valori possibili di $(m-r)$ sono $(m-1), (m-2), \dots, (m-(m-1))=1$; inoltre, se si effettua la sottrazione $a-(m-r)$, ricordando che $(-a)=m*q+r$ cioè $a=(-m*q-r)$, si avrà:

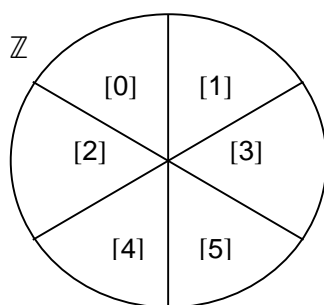
$a-(m-r)=(-m*q-r)-(m-r)=m*(-q-1)$ e, essendo $(-q-1) \in \mathbb{Z}$ si trova che a è della forma $a=m*k$ con $k \in \mathbb{Z}$ e quindi $a \equiv (m-r) \pmod{m}$ e, sempre per il lemma, $[a]=[m-r]$ cioè, essendo $(m-r)$ compreso tra 1 ed $(m-1)$, è una delle classi $[1],[2],\dots,[m-1]$.

La prima parte del teorema è quindi dimostrata.

b) Dimostriamo che le classi $[0],[1],[2],\dots,[m-1]$ sono tutte diverse tra loro. Procediamo per assurdo ipotizzando che due di esse coincidano, ad esempio $[r]=[s]$ con r,s compresi tra 0 e $(m-1)$ ed $r>s$ (se $r<s$ si ragiona in maniera analoga); da $[r]=[s]$ segue (per il lemma) che $r\equiv s \pmod{m}$, cioè $r-s=m\cdot k$, con $k\in\mathbb{Z}$. Essendo $r>0$ ed r,s compresi tra 0 ed $(m-1)$, si avrebbe $0<(r-s)<m$ ed inoltre $(r-s)$ multiplo di m ($(r-s)=m\cdot k$), ma qualsiasi multiplo di m non può essere compreso tra 0 ed $(m-1)$, quindi l'ipotesi fatta per assurdo ci porta ad una contraddizione per cui la seconda parte del teorema è dimostrata.

Esempio di applicazione del teorema: studiamo le classi di congruenza modulo $m=6$.

Per il teorema prima dimostrato, le classi di congruenza modulo 6 sono tutte e sole le classi $[0],[1],[2],[3],[4],[5]$ e sono in totale in numero di 6. Graficamente:



Siamo anche certi che \mathbb{Z} sia diviso in 6 *fette* e che le classi non hanno elementi in comune tra loro.

$$[0]=\{x\in\mathbb{Z} / x=0+6k, \text{ con } k\in\mathbb{Z}\}=\{0,6,12,-6,-12,\dots\}$$

$$[1]=\{x\in\mathbb{Z} / x=1+6k, \text{ con } k\in\mathbb{Z}\}=\{1,7,13,-5,-11,\dots\} \text{ etc.}$$

Vogliamo ora verificare a quale classe coincide $[153]$. Basta seguire la dimostrazione del teorema per il caso $a\geq 0$ ($a=153>0$) e quindi dividere a per il modulo e considerare il resto: $153=6\cdot 25+3$ cioè $[153]=[3]$ (cioè nell'insieme $[3]$ ci sarà anche il numero 153).

Verifichiamo il caso $a<0$, ad esempio $[-81]$: sempre dalla dimostrazione del teorema, dobbiamo questa volta considerare il resto dalla divisione $(-a)=m\cdot q+r$, cioè $81=6\cdot 13+3$; essendo nel caso $r\neq 0$ la classe da considerare è $[m-r]$ cioè $[6-3]=[3]$ da cui $[-81]=[3]$.

Un ulteriore esempio è $[120]$: $120=6\cdot 20+0$, $r=0$ quindi $[120]=[0]$.

Esercizi:

1. data la congruenza modulo $m=11$ trovare con quali classi coincidono le seguenti: $[176]$, $[-35]$ e $[-121]$.

2. se si permettesse che il modulo m fosse 0 oppure 1, cosa potrebbe avvenire per la congruenza modulo 0 e per la congruenza modulo 1? Quante sono le classi? Quanti elementi contiene ogni classe?

Svolgimento.

1. $176 = 11 \cdot 16 + 0 \Rightarrow [176] = [0]$; $35 = 11 \cdot 3 + 2 \Rightarrow [-35] = [11 - 2 = 9]$; $121 = 11 \cdot 11 + 0 \Rightarrow [-121] = [0]$;
2. nel caso modulo 0 la definizione di classe si ha da $P(x,y) = "x-y=0 \cdot k"$ cioè solo se $x=y$, quindi si potrebbero costruire infinite classi con un solo elemento (non valgono più i teoremi dimostrati).

Nel caso $m=1$ la definizione di classe si ha da $P(x,y) = "x-y=1 \cdot k"$ cioè tutti i numeri interi sono congrui modulo 1 tra loro: si avrebbe quindi una sola classe $[x] = \mathbb{Z}$, con infiniti elementi. Anche in questo caso non varrebbero i teoremi dimostrati, tranne il fatto che le classi sono in numero di m .

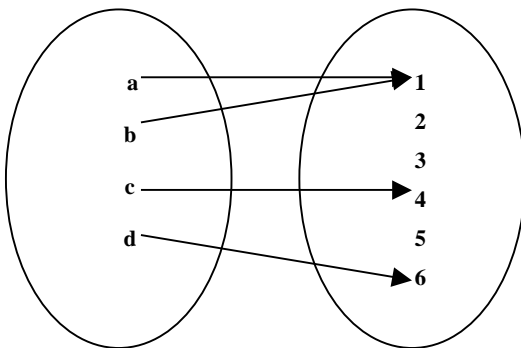
Lezione n°. 21 – 6 dic. 2000

Applicazioni.

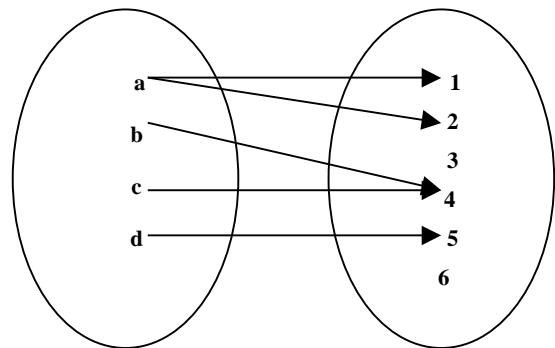
Sia R una relazione dall'insieme A all'insieme B (cioè una regola che associa elementi di A con elementi di B). La relazione R è detta **applicazione (o funzione) da A a B** se, ad ogni elemento di A è associato uno ed uno solo elemento di B (notare che può avvenire sia che qualche elemento di B non sia associato con nessun elemento di A , sia che due o più elementi di A siano associati con lo stesso elemento di B).

Se R è rappresentata graficamente (usando i diagrammi di Eulero-Venn e delle frecce), la R è un'applicazione quando da ogni elemento di A parte una sola freccia (che arriva su un elemento di B).

Esempio:

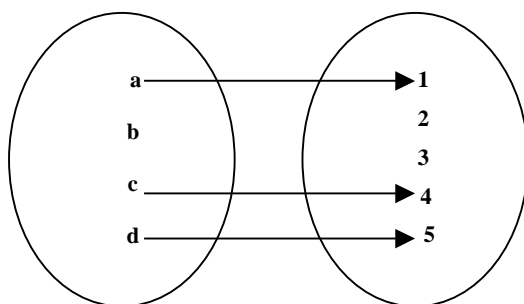


Questa è un'applicazione da A a B .



Questa non è un'applicazione, perché ad $a \in A$ sono associati due elementi di B .

Deve anche avvenire che ogni elemento di A si associato ad un elemento di B.



Questa non è una applicazione da A a B perché l'elemento $b \in A$ non è associato a nessun elemento di B.

Se R è rappresentata con una matrice, dove le righe corrispondono agli elementi di A e le colonne agli elementi di B, la relazione R sarà un'applicazione quando ogni riga contiene esattamente un solo valore 1.

	1	2	3	4	5
a	0	1	0	0	0
b	1	0	0	0	0
c	0	1	0	0	0
d	0	0	0	1	0

Questa matrice corrisponde ad un'applicazione da A a B. Una matrice nella quale una riga contiene tutti zeri oppure 2 o più valori 1 non rappresenta un'applicazione.

Rappresentazione di un'applicazione mediante una formula.

Un'applicazione da A a B, in genere, si indica con una lettera minuscola (spesso f) e, in tale caso, si usa la simbologia $f: A \rightarrow B$. L'insieme A si chiama **dominio dell'applicazione (funzione)** e l'insieme B si chiama **codominio dell'applicazione (funzione)**. Se si considera un elemento $a \in A$, l'unico elemento di b associato ad a è indicato con la simbologia $f(a)$ (detto **immagine di a**). Per definire un'applicazione $f: A \rightarrow B$ spesso si usa una formula del tipo $f(x) =$ (formula che coinvolge la x) con x variabile in A, intendendo che, se si considera un elemento $a \in A$, per calcolare l'immagine $f(a) \in B$ si sostituisce a al posto della x nella formula.

Esempio:

$f: \mathbb{Z} \rightarrow \mathbb{Q}$ (con \mathbb{Q} indichiamo l'insieme dei numeri razionali relativi).

$$f(x) = (x-3)/5$$

Si è così definita un'applicazione f da \mathbb{Z} in \mathbb{Q} intendendo che, se $a \in \mathbb{Z}$, la sua immagine in \mathbb{Q} sarà $f(a) = (a-3)/5$.

Se, ad esempio $a=7$ si ha $f(7) = (7-3)/5 = 4/5$, se $a=-2$ si ha $f(-2) = (-2-3)/5 = -1$.

Non è detto che ogni formula del tipo $f(x) = (\text{formula})$ determini un'applicazione.

Esempio:

$f: \mathbb{Z} \rightarrow \mathbb{Q} \quad f(x) = (5x-3)/(x-2)$ non determina un'applicazione da \mathbb{Z} in \mathbb{Q} perché non si può definire l'immagine di 2, visto che $f(2)$ è una espressione che non si può determinare. Se si restringe il dominio, escludendo il valore 2 si ottiene una applicazione da $\mathbb{Z} - \{2\}$ in \mathbb{Q} :

$f: \mathbb{Z} - \{2\} \rightarrow \mathbb{Q} \quad f(x) = (5x-2)/(x-2)$ che è un'applicazione.

Un altro caso in cui non si determina un'applicazione si ha quando un elemento del dominio può avere due immagini nel codominio.

Esempio:

$f: \mathbb{N} \rightarrow \mathbb{R} \quad f(x) = \pm \sqrt{x}$ non determina un'applicazione da \mathbb{N} ad \mathbb{R} perché per ogni $x \in A$ possiamo avere due immagini $(+\sqrt{x})$ o $(-\sqrt{x})$.

Regola: se l'applicazione è determinata da una formula $f(x) = (\text{formula in } x)$ si deve verificare che per ogni elemento a del dominio la sostituzione di a alla x dia un elemento del codominio e che esso sia unico.

Esercizi:

1. determinare quali delle seguenti relazioni sono applicazioni:

- $f: \mathbb{Z} \rightarrow \mathbb{Z} \quad f(x) = 2x-3$
- $f: \mathbb{P} \rightarrow \mathbb{Z} \quad f(x) = (5x+8)/2$ (\mathbb{P} = insieme dei numeri naturali pari).
- $f: \mathbb{Z} \rightarrow \mathbb{Z} \quad f(x) = (3x-1)/5$

2. fissata la retta r nel piano, siano A l'insieme delle rette perpendicolari ad r e B l'insieme di tutti i punti del piano. Verificare se si ottiene un'applicazione $f: A \rightarrow B$ definendo $f(x) = x \cap r$ (intersezione tra x ed r).

Svolgimento:

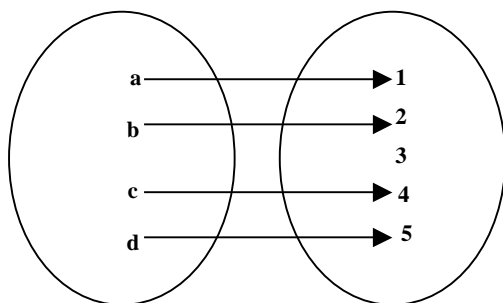
1. a. per ogni valore di $x \in \mathbb{Z}$ si avrà un numero intero distinto di $f(x)$, per cui la relazione è una applicazione di \mathbb{Z} in \mathbb{Z} .
b. per ogni valore di $x \in \mathbb{P}$ si otterrà sempre un numero intero relativo per cui la relazione è un'applicazione da \mathbb{P} in \mathbb{Z} .
c. poiché ci sono dei valori di $x \in \mathbb{Z}$ per i quali la formula non restituisce un numero intero (ad esempio, $f(1)=(3-1)/5=2/5 \notin \mathbb{Z}$, la relazione non è un'applicazione da \mathbb{Z} in \mathbb{Z} .
2. L'immagine di $x \in A$ sarà il punto di intersezione tra la retta x e la retta r , che per ogni retta esiste ed è uno solo: si può allora dire che la relazione è un'applicazione da A in B .

Lezione n°. 22 – 18 dic. 2000

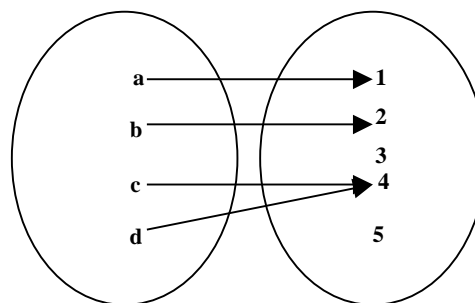
Applicazioni iniettive.

Un'applicazione $f: A \rightarrow B$ si dice **iniettiva** se elementi diversi dell'insieme A hanno sempre elementi corrispondenti diversi nell'insieme B (non devono quindi esistere due elementi diversi di A con lo stesso corrispondente in B).

Graficamente, non devono esistere due frecce che partano da due elementi diversi di A ed arrivino sullo stesso elemento di B .



Iniettiva.



Non iniettiva.

Se l'applicazione è rappresentata in forma matriciale, se essa è iniettiva, non deve esserci più di un valore 1 per ogni colonna (uno e non più di uno per riga, in ogni caso). Potrebbero anche esserci colonne senza alcun valore 1, cioè, se b_c è l'elemento corrispondente alla colonna in questione, potrebbe succedere che b_c non sia corrispondente di alcun valore di A).

	1	2	3	4	5
a	0	1	0	0	0
b	1	0	0	0	0
c	0	1	0	0	0
d	0	0	0	1	0

Nell'esempio, l'applicazione non è iniettiva perché a e c \hat{I} A hanno lo stesso corrispondente $2\hat{I}$ B.

Se l'applicazione $f: A \rightarrow B$ è data con una formula del tipo $f(x)=\dots\dots$, si deve verificare che, presi comunque due elementi $a_1, a_2 \in A$, con $a_1 \neq a_2$, i loro corrispondenti $f(a_1), f(a_2) \in B$ siano tali che $f(a_1) \neq f(a_2)$. In generale si procede con il seguente metodo: si suppone per assurdo che sia $f(a_1)=f(a_2)$ e si cerca di arrivare ad una contraddizione, che spesso consiste nell'arrivare alla conclusione che $a_1=a_2$.

Esempio: $f: \mathbb{Z} \rightarrow \mathbb{Q}$, $f(x)=(3x+5)/7$. perché f sia iniettiva, presi comunque $a_1, a_2 \in \mathbb{Z}$, con $a_1 \neq a_2$, si deve verificare anche $f(a_1) \neq f(a_2)$. Per assurdo, supponiamo che $f(a_1)=f(a_2)$; se così fosse, si avrebbe $(3a_1+5)/7=(3a_2+5)/7$, da cui, moltiplicando ambo i membri per 7, sottraendo 5 ad ambo i membri e dividendoli per 3, si ottiene $a_1=a_2$, che contraddice l'ipotesi, per cui la f è iniettiva.

Cardinalità di un insieme.

Se A è un insieme, il numero dei suoi elementi è detto **cardinalità** (o anche **ordine**) di A ed è indicato con la simbologia $|A|$ (oppure con $\#A$).

Esempi: se $A=\{4,5,6\}$ si ha $|A|=3$. $|\mathbb{Z}|=\infty$.

Teorema: se due insiemi A e B sono finiti e se esiste una applicazione iniettiva $f: A \rightarrow B$ allora $|A| \leq |B|$.

Dimostrazione: supponiamo che gli elementi distinti di A e di B siano:

$A=\{a_1, a_2, \dots, a_t\}$ e $B=\{b_1, b_2, \dots, b_s\}$, quindi che $|A|=t$ e $|B|=s$.

Per ipotesi, essendo f iniettiva, i corrispondenti $f(a_1), f(a_2), \dots, f(a_t)$ di tutti gli elementi di A sono elementi distinti di B e sono in numero di t , quindi B contiene *almeno* t elementi, per cui $s \geq t$ e $|A| \leq |B|$.

Una conseguenza di questo teorema è il principio dei cassetti.

Principio dei cassettei: se A e B sono insiemi finiti, e se $|A| > |B|$, comunque data un'applicazione $f: A \rightarrow B$, esistono sempre due elementi distinti di A che hanno lo stesso corrispondente in B .

Dimostrazione: per il teorema precedente, sicuramente l'applicazione non sarà mai iniettiva, quindi si ha già la tesi.

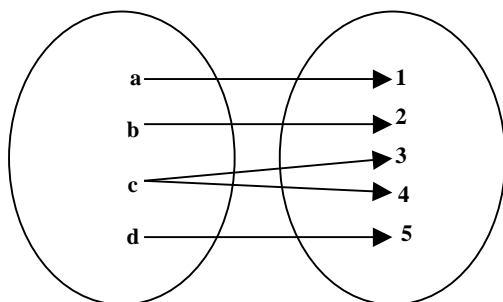
Si usa il termine *cassetti* perché si possono interpretare A come un insieme di oggetti, B come un insieme di cassettei e $f: A \rightarrow B$ come la *legge* che permette di riporre ogni oggetto in un cassetto; il principio dice che, se il numero di oggetti è maggiore del numero dei cassettei, forzatamente due oggetti diversi finiranno nello stesso cassetto.

Esempio: sia dato un insieme di individui A , con la proprietà che alcuni si conoscono tra loro ed altri no (per conoscenza si intende reciproca). Allora esistono sempre almeno due persone del gruppo che hanno lo stesso numero di conoscenti nel gruppo stesso. Infatti: sia $t=|A|$ (numero di persone nel gruppo); costruiamo un insieme B di *cassetti* numerati da 0 a $t-1$ (in totale t cassettei), definiamo un'applicazione $f: A \rightarrow B$ nel modo seguente: associamo ad ogni persona il numero di cassettei corrispondente al numero di conoscenti della persona stessa (0 se non conosce nessuno, $t-1$ se conosce tutti ($t-1$ perché è tutto il gruppo tranne se stesso)). È ovvio che se c'è una persona nel cassetto 0, non ci sarà nessuna persona nel cassetto $t-1$ e viceversa (se una persona non conosce nessuno non c'è nessuno che conosce tutti e viceversa). Quindi almeno uno tra i cassettei 0 e $t-1$ sarà vuoto. Eliminiamo il cassetto vuoto ed otteniamo quindi un insieme B_0 tale che $|B_0|=t-1$. Se riappliciamo la stessa applicazione f dall'insieme A al nuovo insieme B_0 , per il principio dei cassettei, essendo $t-1=|B_0| < |A|=t$, esisteranno almeno due persone associate allo stesso cassetto, cioè avranno lo stesso numero di conoscenti all'interno del gruppo.

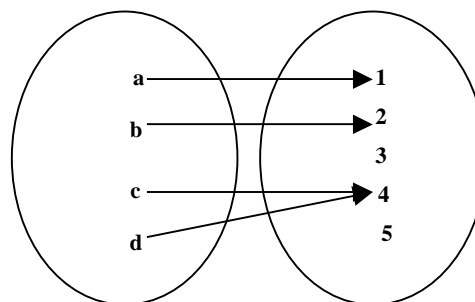
Applicazioni surgettive.

Se $f: A \rightarrow B$ è un'applicazione dall'insieme A all'insieme B, f è detta **surgettiva** se ogni elemento di B è il corrispondente di almeno un elemento di A.

Graficamente, ogni elemento di B deve essere l'estremo di almeno una freccia.



Surgettiva.



Non surgettiva.

Se l'applicazione è rappresentata in forma matriciale, se essa è surgettiva, in ogni colonna deve esserci almeno un valore uguale ad 1. Non possono esserci colonne senza alcun valore 1, cioè con tutti i valori uguali a 0.

	1	2	3	4	5
a	0	1	0	0	0
b	1	0	1	0	0
c	0	1	0	0	0
d	0	0	0	1	0

Nell'esempio, l'applicazione non è surgettiva perché l'elemento 5 di B non è corrispondente di nessun elemento di A (colonna con valori tutti nulli).

Se l'applicazione $f: A \rightarrow B$ è data con una formula del tipo $f(x)=\dots\dots$, si deve verificare che, preso comunque un elemento $b \in B$, esista almeno un elemento $x \in A$ tale che $f(x)=b$. L'espressione $f(x)=b$ diventa un'equazione nell'incognita x: se esiste una soluzione in A, la f è surgettiva.

Esempi:

- $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x)=x+5$. Verifichiamo se f è surgettiva: si prende un qualunque elemento $b \in \mathbb{Z}$ (insieme di arrivo) e si deve trovare almeno una soluzione $x \in \mathbb{Z}$ (insieme di partenza)

tale che $f(x)=x+5=b$, cioè risolvere l'equazione $x+5=b$ (b è un valore noto). Nel nostro caso allora $x=b-5$ e $x \in \mathbb{Z}$ perché $b \in \mathbb{Z}$, quindi x è la differenza di due interi relativi che è ancora un intero relativo. La f è allora surgettiva.

- $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x)=3x-1$. L'equazione da risolvere è: $3x-1=b$ che ha come soluzione $x=(b+1)/3$. In questo caso non sempre x è un intero relativo (può essere anche un razionale) per cui la f non è surgettiva.

Teorema: se A e B sono insiemi finiti e se esiste un'applicazione surgettiva $f: A \rightarrow B$ allora $|A| \geq |B|$. (confrontare con l'analogo teorema per le applicazioni iniettive).

Dimostrazione: supponiamo che gli elementi distinti di A e di B siano:

$A=\{a_1, a_2, \dots, a_r\}$ e $B=\{b_1, b_2, \dots, b_s\}$, quindi che $|A|=r$ e $|B|=s$.

Per ipotesi, essendo f surgettiva, preso $b_1 \in B$ esiste almeno un elemento $c_1 \in A$ tale che $f(c_1)=b_1$. Allo stesso modo, preso $b_2 \in B$ esiste almeno un elemento $c_2 \in A$ tale che $f(c_2)=b_2$. Ripetendo lo stesso ragionamento per ogni elemento di B , alla fine si avrà che, preso $b_s \in B$ esiste almeno un elemento $c_s \in A$ tale che $f(c_s)=b_s$. Ma c_1, c_2, \dots, c_s sono elementi distinti (se, per assurdo, fosse $c_1=c_2$ tale elemento avrebbe due corrispondenti b_1 e b_2 distinti e ciò andrebbe contro la definizione di applicazione). Si sono quindi trovati s elementi in A , che costituiscono il dominio della f . Poiché essi sono almeno s elementi (f è surgettiva), ne deriva che $|A| \geq |B|$.

Conseguenze: se A e B sono insiemi finiti e se $|A| < |B|$ non esistono applicazioni surgettive $f: A \rightarrow B$.

Lezione n°. 24 – 8 gen. 2001

Correzione esercizi lasciati per casa.

Lezione n°. 25 – 10 gen. 2001

Applicazioni biunivoche.

Se l'applicazione $f: A \rightarrow B$ è sia iniettiva che surgettiva è detta **biunivoca**.

Conseguenze della biunivocità di una applicazione.

Se A e B sono due insiemi finiti e se $f: A \rightarrow B$ è una applicazione biunivoca, si ha:

$|A| \leq |B|$ (perché è iniettiva) e $|A| \geq |B|$ (perché è surgettiva) quindi $|A|=|B|$, cioè i due insiemi hanno lo stesso numero di elementi. Quindi, quando A e B sono due insiemi finiti e $|A| \neq |B|$, non esistono applicazioni biunivoche $f: A \rightarrow B$.

Il concetto di applicazione biunivoca è alla base del “*contare*”.

Esempio: se è dato l'insieme $A=\{a,b,c,d\}$, allora, per contare il numero di elementi di A , si costruisce un'applicazione biunivoca da A all'insieme $B=\{1,2,3,4\}$.

Per contare il numero di elementi di un insieme finito A può essere utile costruire un'applicazione biunivoca $f: A \rightarrow B$, dove B è un insieme finito nel quale è più *facile* contare il numero di elementi.

Esempio: si consideri il seguente insieme di numeri interi relativi

$A=\{x \in \mathbb{Z} / -17 < x \leq 823 \text{ e } x \equiv 3 \pmod{5}\}$. Si vuole conoscere $|A|$.

Si osserva che, dato un elemento $x \in A$, il numero $x+17$ è un intero positivo (perché $x > -17$), e che $x+17 \leq 840$ (perché $x \leq 823$). Inoltre si ha che $(x+17)/5$ è un intero perché $x \equiv 3 \pmod{5}$ significa che $x-3=5*k$ (con $k \in \mathbb{Z}$) da cui si ricava $x=3+5*k$ da cui, sommando 17 e dividendo per 5 si ottiene che $(x+17)/5=(20+5*k)/5=4+k$ che è un numero intero. Allora, avendo trovato che $0 < (x+17) \leq 840$, se dividiamo tutto per 5 otteniamo $0 < (x+17)/5 \leq 168$. In pratica, con questo ragionamento, si può definire un'applicazione $f: A \rightarrow B$ (dove B è l'insieme dei numeri naturali ≤ 168) con $f(x)=(x+17)/5$. Si verifica facilmente che la f è un'applicazione biunivoca. Infatti è iniettiva perché se, per assurdo, ipotizziamo che esistano $a,b \in A$ tali che $f(a)=f(b)$, con $a \neq b$, otteniamo $(a+17)/5=(b+17)/5$, da cui, moltiplicando per 5 e sottraendo 17 si otterrebbe $a=b$, in contraddizione con l'ipotesi $a \neq b$. Inoltre è surgettiva perché, comunque preso $z \in B$, da $z=(x+17)/5$ si ottiene $x=5*z-17$ che appartiene sempre all'insieme A (essendo $1 < z \leq 168$). La biunivocità dell'applicazione $f: A \rightarrow B$ ci consente di dire che $|A|=|B|=168$.

Esercizio: contare quanti sono i numeri interi positivi di 5 cifre decimali ($10000 \leq x \leq 99999$) che hanno la cifra centrale uguale a 3.

Svolgimento: isoliamo la cifra centrale e consideriamo come variano le altre cifre. Eccetto la cifra più significativa che potrà variare da 1 a 9 (non 0 perché il numero deve essere di 5 cifre), le altre possono variare da 0 a 9, quindi si avranno tutti i numeri da 0 a 9999, che sono in tutto 9000 ($9 * 1000$ che sono le possibili combinazioni delle altre tre cifre). Allora i numeri decimali a cinque cifre con cifra centrale 3 sono 9000.

Applicazione identica (o identità).

Se A è un insieme finito qualunque (non vuoto) si può costruire un'applicazione $f: A \rightarrow A$ ponendo $f(x)=x$ (associando cioè ad ogni elemento di A se stesso), che si chiama *applicazione identica* (o *identità*), ed è ovviamente un'applicazione biunivoca.

Applicazione inversa.

Se $f: A \rightarrow B$ è un'applicazione biunivoca, preso un generico $x \in B$, la surgettività garantisce che esiste almeno un elemento $y \in A$ tale che $f(y)=x$; l'iniettività garantisce inoltre che questo elemento $y \in A$ è unico. Possiamo quindi costruire (quando l'applicazione è biunivoca) un'applicazione, detta *applicazione inversa di f* , che si indica con $f^{-1}: B \rightarrow A$, che associa ad ogni elemento $x \in B$ quell'unico elemento $y \in A$ tale che la sua immagine mediante la $f: A \rightarrow B$ sia x .

Se la $f: A \rightarrow B$ è definita graficamente, la sua inversa $f^{-1}: B \rightarrow A$ si ottiene invertendo il verso delle frecce.

Se la $f: A \rightarrow B$ è definita in forma matriciale, la sua inversa $f^{-1}: B \rightarrow A$ si ottiene scambiando le righe con le colonne e viceversa (l'intestazione delle colonne diventa A e quella delle righe diventa B).

Se la $f: A \rightarrow B$ è definita mediante una formula, per definire la sua inversa $f^{-1}: B \rightarrow A$, si prende un generico elemento $x \in B$ e si osserva che $f^{-1}(x)$ è quell'unico elemento $y \in A$ tale che $f(y)=x$. Da questa scrittura si ricava y in funzione di x e quindi si pone $f^{-1}(x)=y=(\text{formula})$.

Esempio: sia data l'applicazione biunivoca la $f: \mathbb{Z} \rightarrow \mathbb{Z}$ definita dalla formula $f(x)=x+5$. Per costruire l'inversa $f^{-1}: \mathbb{Z} \rightarrow \mathbb{Z}$ si prende un generico elemento $x \in \mathbb{Z}$ e si osserva che $f^{-1}(x)$ è quell'unico $y \in \mathbb{Z}$ tale che $f(y)=x$, cioè: $y+5=x$, da cui si ottiene $y=x-5$. Allora l'inversa dell'applicazione f è $f^{-1}: \mathbb{Z} \rightarrow \mathbb{Z}$ definita dalla formula $f^{-1}(x)=x-5$.

Esercizio: dati l'insieme A dei numeri reali >2 e l'insieme B dei numeri reali >0 e l'applicazione $f: A \rightarrow B$ definita dalla formula $f(x)=+\sqrt{x-2}/7$, dimostrare che f è un'applicazione biunivoca e calcolare l'applicazione inversa di f .

Svolgimento: verifichiamo l'iniettività della f . Supponiamo per assurdo che, presi $a, b \in A$, con $a \neq b$, si verifichi $f(a)=f(b)$; si avrebbe allora $+\sqrt{a-2}/7 = +\sqrt{b-2}/7$. Moltiplicando per 7 ed

elevando entrambi i membri al quadrato si otterrebbe $a^2=b^2$, cioè $a=b$ che contraddice l'ipotesi $a \neq b$, quindi l'applicazione è iniettiva. Verifichiamo adesso la surgettività: preso un qualunque $z \in B$, da $z = \frac{\sqrt{x-2}}{7}$, si ottiene $x=49z^2+2$, che è un numero reale >2 e quindi appartiene ad A . L'applicazione è quindi anche surgettiva e quindi è biunivoca.

Troviamo ora l'applicazione inversa $f^{-1}: B \rightarrow A$. Abbiamo già visto che, preso un generico elemento x di B , l'unico elemento y di A tale che $f(y)=x$ è $y=49x^2+2$, per cui l'applicazione inversa di f , $f^{-1}: B \rightarrow A$ sarà definita dalla formula $f^{-1}(x)=49x^2+2$.

Lezione n°. 26 – 12 gen. 2001

Teorema: se A e B sono due insiemi finiti e se $f: A \rightarrow B$ è un'applicazione allora, se $|A|=|B|$ si ha che f è iniettiva $\Leftrightarrow f$ è surgettiva (in pratica se l'applicazione f è iniettiva automaticamente sarà anche surgettiva quindi biunivoca).

Dimostrazione: siano a_1, a_2, \dots, a_n gli elementi distinti dell'insieme A (quindi $|A|=n$). supponiamo che l'applicazione f sia iniettiva e dimostriamo che essa sarà anche surgettiva. L'iniettività garantisce che i corrispondenti $f(a_1), f(a_2), \dots, f(a_n)$ sono anch'essi elementi distinti dell'insieme B . Allora tali corrispondenti sono n elementi di B che, per ipotesi, contiene proprio n elementi, e quindi tali corrispondenti esauriscono l'insieme B e da ciò segue che la f è surgettiva, visto che ogni elemento di B è corrispondente di un elemento di A .

Supponiamo adesso l'applicazione f surgettiva e dimostriamo che sarà anche iniettiva. Se, per assurdo, la f non fosse iniettiva, esisterebbero elementi distinti di A con uguale corrispondente in B . Ma ciò comporterebbe che i corrispondenti $f(a_1), f(a_2), \dots, f(a_n)$ fossero in numero minore di n e quindi non coprirebbero l'insieme B , in contraddizione con l'ipotesi della surgettività della f . L'applicazione f è allora anche iniettiva ed il teorema è dimostrato.

Schematicamente, per gli insiemi finiti, si può riassumere che, se $|A|=n$ e $|B|=m$, allora:

1. se $n < m$ esistono applicazioni $f: A \rightarrow B$ iniettive ma non surgettive;
2. se $m < n$ esistono applicazioni $f: A \rightarrow B$ surgettive ma non iniettive;
3. se $m = n$ esistono applicazioni $f: A \rightarrow B$ iniettive e surgettive, cioè biunivoche.

Cerchiamo ora di *contare* le applicazioni tra insiemi finiti.

Se A e B sono insiemi finiti e se $|A|=n$ e $|B|=m$, contiamo quante sono le possibili applicazioni $f: A \rightarrow B$.

Se $A=\{a_1, a_2, \dots, a_n\}$ e $B=\{b_1, b_2, \dots, b_m\}$, per costruire un'applicazione si deve scegliere il corrispondente $f(a_1) \in B$ di a_1 tra le m scelte possibili; per ognuna di queste m scelte, ci sono m possibilità di scelta per il corrispondente di a_2 (stiamo parlando di applicazioni generiche). In totale avremo quindi $m \cdot m$ scelte possibili per $f(a_1)$ ed $f(a_2)$. Ripetendo il ragionamento per tutti gli altri corrispondenti $f(a_3), f(a_4), \dots, f(a_n)$, alla fine avremo $m \cdot m \cdot \dots \cdot m = m^n$ scelte possibili. In conclusione, se $|A|=n$ e $|B|=m$ il numero totale di applicazioni generiche $f: A \rightarrow B$ è di m^n .

Esempio:

Se $|A|=3$ e $|B|=4$: $A=\{a_1, a_2, a_3\}$ e $B=\{b_1, b_2, b_3, b_4\}$. Per costruire un'applicazione $f: A \rightarrow B$ prima si deve scegliere il corrispondente $f(a_1)$ tra le 4 scelte possibili. Per ognuna di queste 4 scelte possibili si deve scegliere il corrispondente $f(a_2)$. Per ogni scelta fissata per $f(a_1)$ si hanno 4 possibilità di scelta per $f(a_2)$, per un totale di $4 \cdot 4 = 16$. Per ognuna di queste 16 scelte possibili avremo 4 possibilità di scelta per il corrispondente $f(a_3)$, quindi un totale di $4 \cdot 4 \cdot 4 = 64 = 4^3$. Allora il numero di applicazioni generiche possibili $f: A \rightarrow B$, se $|A|=3$ e $|B|=4$, è 4^3 .

Vediamo adesso quante sono le possibili applicazioni iniettive $f: A \rightarrow B$, se A e B sono insiemi finiti e se $|A|=n$ e $|B|=m$.

Dobbiamo distinguere due casi:

1. se $n > m$ non avremo nessuna applicazione iniettiva;
2. se $n \leq m$, per il corrispondente $f(a_1)$ avremo m scelte possibili. Per ognuna di queste m scelte, le possibilità di scelta per il corrispondente $f(a_2)$ sono $m-1$ (essendo f iniettiva, deve essere $f(a_1) \neq f(a_2)$), quindi in totale $m \cdot (m-1)$ scelte possibili per $f(a_1)$ ed $f(a_2)$. Per ognuna di queste $m \cdot (m-1)$ scelte avremo $(m-2)$ possibilità di scegliere $f(a_3)$ e così via fino ad $f(a_n)$ per il quale troveremo $m-(n-1)$ possibilità di scelta. In conclusione le possibili applicazioni iniettive sono in numero di $m \cdot (m-1) \cdot \dots \cdot (m-n+1)$.

Esempio:

Se $|A|=3$ e $|B|=7$, il numero di applicazioni iniettive da A a B è uguale a $7 \cdot 6 \cdot 5 = 210$ (sulle $7^3 = 343$ applicazioni generiche possibili).

Contare quante sono le possibili applicazioni surgettive $f: A \rightarrow B$, se A e B sono insiemi finiti e se $|A|=n$ e $|B|=m$ è molto più complesso.

Anche in questo caso si devono distinguere due casi:

1. se $n < m$ non avremo nessuna applicazione surgettiva;
2. se $n \geq m$ non esiste una formula algebrica come visto per le altre applicazioni. Tale numero viene detto **numero di Stirling**, indicato con $S(n,m)$, e verrà studiato più avanti.

Contiamo infine le applicazioni biunivoche $f: A \rightarrow B$, se A e B sono insiemi finiti e se $|A|=n$ e $|B|=m$.

Naturalmente, se $n \neq m$ non esisteranno applicazioni biunivoche. Se invece $n=m$, in base al teorema dimostrato precedentemente, tutte le applicazioni iniettive sono automaticamente biunivoche per cui basta contare le applicazioni iniettive che sappiamo essere in numero di $m \cdot (m-1) \cdot \dots \cdot (m-n+1)$. Essendo $m=n$ si può scrivere $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1$. Si ottiene cioè il prodotto di tutti i numeri naturali da 1 ad n (estremi compresi). Tale numero è detto **fattoriale di n** e si indica con **$n!$**

Esempio: se $|A|=|B|=5$, le possibili applicazioni biunivoche tra A e B sono $5!=5 \cdot 4 \cdot 3 \cdot 2 \cdot 1=120$.

Lezione n° 27 – 15 gen. 2001

CALCOLO COMBINATORIO.

Disposizioni semplici e con ripetizioni.

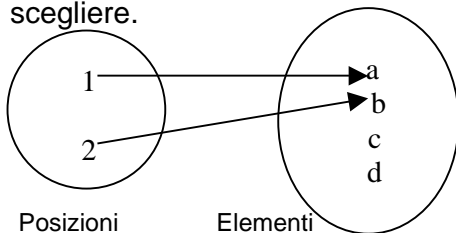
Sia dato un insieme di 4 elementi, $A=\{a,b,c,d\}$ e si considerino tutti i possibili modi di disporre *ordinatamente* due elementi scelti tra i 4. (Con il termine *ordinatamente* si intende che anche l'ordine in cui si prendono gli elementi ha importanza, cioè che, ad esempio, $ab \neq ba$). Avremo: $ab, ba, ac, ca, ad, da, bc, cb, bd, db, cd, dc$. Si ottengono 12 possibili modi di disporre ordinatamente i 4 elementi a 2 a 2.

Si noti che non è stata considerata la possibilità di ripetere più volte lo stesso elemento; se tale possibilità fosse ammessa si otterrebbero altri 4 modi di disporre i 4 elementi a 2 a 2: aa, bb, cc, dd , per un totale di 16 possibili modi.

In generale, dati n elementi di un insieme non vuoto (n è un intero ≥ 1) e fissato un intero k tale che $1 \leq k \leq n$, si chiamano **disposizioni semplici degli n elementi, presi a k a k** , i diversi modi di disporre ordinatamente k elementi *distinti* scelti tra gli n .

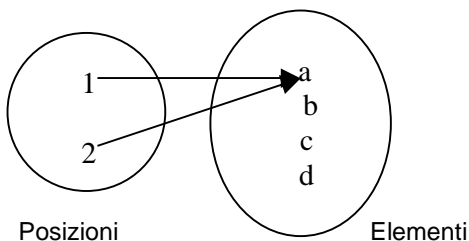
Se invece k è un intero ≥ 1 (senza cioè limite superiore per il suo valore), si chiamano **disposizioni con ripetizione degli n elementi presi a k a k** , i diversi modi di disporre ordinatamente k elementi scelti tra gli n , con la possibilità che un elemento sia ripetuto più di una volta.

In pratica, per fissare una disposizione semplice di 4 elementi presi a 2 a 2, si devono fissare due *posizioni* (posizione 1 e posizione 2), ed inserire in tali posizioni due elementi distinti scelti tra i 4. Allora la costruzione di tali disposizioni semplici equivale alla costruzione di un'applicazione tra l'insieme delle *posizioni* e l'insieme degli elementi da scegliere.



Se si associa la posizione 1 all'elemento a e la posizione 2 all'elemento b si costruisce un'applicazione f tra i due insiemi, ottenendo la disposizione semplice ab .

Tali applicazioni equivalenti alle disposizioni semplici sono iniettive, non essendo ammesse ripetizioni. Invece le disposizioni con ripetizione sono equivalenti ad applicazioni generiche (iniettive e non).



Se si associano sia la posizione 1 che la posizione 2 allo stesso elemento a l'applicazione f equivale alla disposizione con ripetizione aa .

In generale, allora, le disposizioni semplici di n elementi presi a k a k sono equivalenti ad applicazioni iniettive dall'insieme delle posizioni $\{1, 2, \dots, k\}$ all'insieme dato di n elementi $\{a_1, a_2, \dots, a_n\}$. quelle con ripetizione sono invece equivalenti ad applicazioni generiche (iniettive e non) tra gli stessi insiemi. Dalla teoria del calcolo del numero di applicazioni possibili fra due insiemi finiti si deduce che:

1. il numero di disposizioni semplici di n elementi presi a k a k ($1 \leq k \leq n$) è uguale a $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1)$;
2. il numero di disposizioni con ripetizione di n elementi presi a k a k ($k \geq 1$) è uguale a n^k .

Nell'esempio fatto $n=4$ ed $k=2$ si è infatti visto che le disposizioni semplici erano $4 \cdot 3 = 12$ e le disposizioni con ripetizione erano $4^2 = 16$.

Esempi.

- Le colonne possibili del totocalcio.

Una colonna equivale ad una disposizione con ripetizione di 3 elementi $(1, X, 2)$ presi a 13 a 13, quindi il numero di colonne possibili è uguale a $3^{13} = 1.594.323$.

- I numeri interi >0 che, scritti in base 10, usano solo 3 cifre e tutte dispari.
Tali numeri sono le disposizioni con ripetizione di 5 elementi (1,3,5,7,9) presi a tre a tre, quindi $5^3=125$. Se si impone che le cifre siano distinte si ottiene che tali numeri sono $5*4*3=60$ disposizioni semplici.

Combinazioni semplici.

Vi sono problemi in cui si combinano k elementi scelti tra gli n totali ma senza che l'ordine in cui siano presi abbia importanza (ad esempio un cinquina al lotto). Si chiamano ***combinazioni semplici di n elementi presi a k a k ($1 \leq k \leq n$)*** i diversi modi di combinare k elementi scelti tra gli n dati senza ripetizione e senza importanza per l'ordine. In pratica, una combinazione semplice di n elementi presi a k a k non è altro che un sottoinsieme di k elementi (cioè di ordine k) estratto da un insieme *totale* di n elementi (cioè di ordine n).

Esempio: se $n=4$, $A=\{a,b,c,d\}$ e $k=3$ le combinazioni semplici di 4 elementi presi a 3 a 3 sono i sottoinsiemi di ordine 3 estratti dall'insieme A :

$\{a,b,c\}, \{a,c,d\}, \{a,b,d\}, \{b,c,d\}$ in tutto 4 combinazioni semplici.

Identificando le combinazioni semplici di n elementi presi a k a k con i sottoinsiemi di ordine k estratti da un insieme di ordine n , si può dare un significato anche al caso in cui sia $k=0$: vi è soltanto un sottoinsieme di ordine 0, che è l'insieme vuoto, e quindi le combinazioni semplici di n elementi con $k=0$ sono in numero di 1 (cioè il non combinarli, non prenderne nessuno). Il numero totale delle combinazioni semplici di n elementi presi a k a k ($0 \leq k \leq n$) è detto ***coefficiente binomiale*** ed è indicato con il simbolo $\binom{n}{k}$

Dagli esempi fatti si è visto che se $k=0$ si ha che $\binom{n}{k}=1$ e se $n=4$ e $k=3$ $\binom{n}{k}=4$. il problema che si pone è quello di trovare il valore di $\binom{n}{k}$ per qualsiasi valore di n e k .

Lezione n°. 28 – 17 gen. 2001

Determinazione del valore del coefficiente binomiale.

Le disposizioni semplici degli n elementi presi a k a k , nel caso particolare in cui $n=k$, si chiamano ***permutazioni degli n elementi***. Esse sono in numero di $n!$ (infatti sono in numero di $n*(n-1)*(n-2)*\dots*(n-n+1)=n*(n-1)*(n-2)*\dots*1=n!$).

Esempio: se $n=3$, $A=\{a,b,c\}$ le permutazioni si ottengono disponendo gli elementi nei vari ordini possibili: $abc, acb, bac, bca, cab, cba$, che sono in numero di $6=3!$

Fatta questa premessa, cerchiamo di determinare il valore di $\binom{n}{k}$, con k tale che $1 \leq k \leq n$.

Tale numero rappresenta il numero di sottoinsiemi di ordine k estratti dall'insieme di ordine n . consideriamo prima tutte le disposizioni semplici degli elementi presi a k a k , che sappiamo essere in numero di $n*(n-1)*(n-2)*...*(n-k+1)$. Vi saranno alcune di tali disposizioni (quelle che coinvolgono gli stessi k elementi) che corrispondono ad un'unica combinazione.

Esempio: se $n=5$ e $k=3$ e se $A=\{a,b,c,d,e\}$ allora le disposizioni semplici che coinvolgono gli elementi $\{a,b,c\}$ sono: $abc, acb, bca, bac, cab, cba$ e corrispondono tutte all'unica combinazione $\{a,b,c\}$.

Per calcolare il numero totale di combinazioni (cioè il numero $\binom{n}{k}$), si possono raggruppare tutte le disposizioni che coinvolgono gli stessi k elementi (che corrispondono ad un'unica combinazione). In ogni *gruppo* vi sono tutte le disposizioni semplici di k elementi presi a k a k , cioè le permutazioni di questi k elementi, che sono in numero di $k!$. Allora, per trovare il numero di *gruppi*, bisognerà dividere il numero totale di disposizioni semplici di n elementi presi a k a k (che è uguale a $n*(n-1)*(n-2)*...*(n-k+1)$) per il numero di permutazioni di ogni gruppo ($k!$). Possiamo allora scrivere:

$$\binom{n}{k} = \frac{n*(n-1)*(n-2)*...*(n-k+1)}{k!} \quad \text{con } 1 \leq k \leq n.$$

Questo numero è un numero intero, essendo un numero di combinazioni.

Esiste anche una seconda formula, equivalente a quella trovata, che risulta più compatta e che si ottiene moltiplicando numeratore e denominatore per lo stesso numero $(n-k)!$.

In definitiva, abbiamo due formule equivalenti per il valore del coefficiente binomiale:

$$\binom{n}{k} = \frac{n*(n-1)*(n-2)*...*(n-k+1)}{k!} * \frac{(n-k)!}{(n-k)!} = \frac{n*(n-1)*...*(n-k+1)*(n-k)*(n-k-1)*...*1}{k!*(n-k)!} = \frac{n!}{k!(n-k)!}$$

$$\binom{n}{k} = \frac{n*(n-1)*(n-2)*...*(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Esempi:

1. I sottoinsiemi di ordine 4 estratti da un insieme di ordine 10 sono in numero di

$$\binom{10}{4} = \frac{10*9*8*7}{4*3*2} = 210$$

Notare che tutti i sottoinsiemi dell'insieme di ordine 10 sono in numero di $2^{10}=1024$.

2. Le possibili cinque al gioco del lotto sono le combinazioni semplici di 90 elementi

$$\text{presi a 5 a 5 quindi: } \binom{90}{5} = \frac{90*89*88*87*86}{5*4*3*2} = 43.949.268$$

3. I diversi 6 al gioco del superenalotto sono in numero di:

$$\binom{90}{6} = \frac{90 * 89 * 88 * 87 * 86 * 85}{6 * 5 * 4 * 3 * 2} = 622.614.630$$

Consideriamo adesso tutti i possibili coefficienti binomiali con n noto (ad esempio n=5, e quindi $1 \leq k \leq 5$) ed aggiungiamo anche il caso k=0 per il quale il coefficiente binomiale assume valore 1 (per k=0 la formula trovata non vale, lo si dà per definizione, visto che esso corrisponde al sottoinsieme *insieme vuoto*). Otterremo:

$$\binom{5}{0} = 1 \quad \binom{5}{1} = 5 \quad \binom{5}{2} = 10 \quad \binom{5}{3} = 10 \quad \binom{5}{4} = 5 \quad \binom{5}{5} = 1$$

Si nota che i coefficienti binomiali sono uguali a coppie simmetriche rispetto al centro della successione. Ciò deriva da una formula generale

$$\binom{n}{k} = \binom{n}{n-k}$$

Quindi, ad esempio: $\binom{5}{2} = \binom{5}{5-2} = \binom{5}{3}$

Se n è pari si avrà un coefficiente binomiale centrale che non può essere *accoppiato* con nessun altro, però la simmetria a coppie rimane.

Dimostriamo questa formula; distinguiamo due casi:

1. k=0:

$$\binom{n}{k} = \binom{n}{0} = 1$$

$$\binom{n}{n-k} = \binom{n}{n-0} = \binom{n}{n} = 1$$

Per il caso k=0 l'uguaglianza è provata.

2. k≠0: possiamo usare la seconda formula del coefficiente binomiale.

$$\binom{n}{n-k} = \frac{n!}{(n-k)! (n-(n-k))!} = \frac{n!}{(n-k)! (n-n+k)!} = \frac{n!}{(n-k)! k!} = \binom{n}{k}$$

Esercizio: quanto vale la somma di tutti i possibili coefficienti binomiali?

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n}$$

Svolgimento: in generale, $\binom{n}{k}$ indica il numero di sottoinsiemi di ordine k estratti da un insieme di ordine n. La somma di tutti i coefficienti binomiali (con $0 \leq k \leq n$) non è altro che il numero di tutti i sottoinsiemi possibili, di qualsiasi ordine, dell'insieme di ordine n e

sappiamo, dalla teoria degli insiemi, che questo numero è pari a 2^n , che rappresenta quindi anche la somma di tutti i coefficienti binomiali.

Lezione n° 29 – 19 gen. 2001

Combinazioni con ripetizione.

Dato un insieme con n elementi, una combinazione con ripetizione degli n elementi presi a k a k , dove k è un numero intero ≥ 1 , è un modo di combinare, indipendentemente dall'ordine, k degli n elementi con possibili ripetizioni.

Esempio: se $n=3$, $\{a,b,c\}$, un esempio di combinazioni con ripetizione dei 3 elementi presi a 7 a 7 può essere aabbbbc (notare che la stessa combinazione può essere scritta con un ordine diverso: abbbbc; l'ordine non ha importanza e le due scritture rappresentano la stessa combinazione con ripetizione).

Quindi una combinazione è individuata dal numero di volte in cui ogni elemento viene preso. Cerchiamo di determinare il numero di combinazioni con ripetizione di n elementi presi a k a k .

Introduciamo prima il concetto di **parola di un alfabeto**; dato un insieme di n elementi (detto **alfabeto**), una *parola* di lunghezza k (con $k \geq 1$) è una qualunque disposizione con ripetizione degli n elementi (detti anche *lettere dell'alfabeto*) presi a k a k . Se l'alfabeto è quello della lingua italiana, una parola di lunghezza 6 è, per esempio, *strada* (ma anche *trsdad* è una *parola* di lunghezza 6). Un alfabeto molto particolare è quello formato dai due simboli $\{0,1\}$: una parola di lunghezza 7 è, per esempio, 0101110. Proviamo a risolvere il seguente problema: determinare il numero di tutte le possibili parole di lunghezza k dell'alfabeto $\{0,1\}$ che contengano un numero fissato m di *lettere* 0 (oppure 1, è la stessa cosa). Per costruire una di tali parole si devono prendere le posizioni possibili delle *lettere* nella parola

--	--	--	--	--	--	--	--

--	--

Si devono quindi fissare m delle k posizioni e, in queste m , mettere il valore (*lettera*) 0 (nelle altre andrà automaticamente la *lettera* 1). Tali scelte possibili delle m posizioni delle *lettere* 0 non sono altro che combinazioni semplici di k elementi presi ad m ad m , e sono allora in numero di $\binom{k}{m}$

Se, ad esempio, volessimo contare le parole dell'alfabeto $\{0,1\}$ di lunghezza 4 che contengano 2 volte la *lettera* 0, dovremmo scegliere 2 posizioni per lo 0 ed il numero di parole possibili è $\binom{4}{2}$, cioè $(24/4=6)$: (0001,0101,0110,1001,1010,1100).

Torniamo al problema della determinazione del numero di combinazioni con ripetizione di n elementi presi a k a k . Gli elementi siano $\{a_1, a_2, a_3, \dots, a_n\}$. Una delle possibili combinazioni si determina prendendo m_1 volte a_1 , m_2 volte a_2 m_n volte a_n (m_i può anche essere 0), con $m_1 + m_2 + m_3 + \dots + m_n = k$. Ad ognuna di tali combinazioni si può associare una parola dell'alfabeto $\{0,1\}$, operando come segue: si metteranno m_1 valori 1 per la lettera a_1 , quindi un valore 0 separatore, poi m_2 valori 1 per la lettera a_2 , e così via fino a m_n valori 1 per la lettera a_n .

Se, ad esempio, $n=4$, $\{a_1, a_2, a_3, a_4\}$, ed $m=8$ alla combinazione $a_1 a_1 a_2 a_2 a_2 a_3 a_4 a_4$ si associa la parola su $\{0,1\}$: 11011101011.

Le parole associate alle combinazioni che vogliamo contare sono parole con un numero di cifre 0 pari a $(n-1)$ ed un numero di cifre 1 pari a k , cioè di lunghezza uguale a $(m+n-1)$. Si verifica facilmente che tale associazione fra combinazioni con ripetizione e parole su $\{0,1\}$ determina un'applicazione biunivoca fra i due insiemi:

***{combinazioni con ripetizioni di n elementi presi a k a k } e
{parole su $\{0,1\}$ di lunghezza $(m+n-1)$ e con $(n-1)$ cifre 0}.***

Allora il numero di combinazioni cercato coincide con quanto visto in precedenza sul numero di parole sull'alfabeto $\{0,1\}$ con un numero fissato di lettere 0, cioè: $\binom{k+n-1}{n-1}$

Ricordando la proprietà del coefficiente binomiale che dice che: $\binom{n}{k} = \binom{n}{n-k}$

Si può anche scrivere che il numero di combinazioni con ripetizione di n elementi presi a k a k è uguale a: $\binom{k+n-1}{k}$

Lezione n°. 30 – 22 gen. 2001

Proprietà del coefficiente binomiale.

Se n è un intero ≥ 1 ed m un intero tale che $0 \leq k \leq n$, il coefficiente binomiale $\binom{n}{k}$ è il numero dei sottoinsiemi di ordine k estratti da un insieme di ordine n (*combinazione semplice*). Fissato n e facendo variare k si ottengono $(n+1)$ coefficienti binomiali:

$$\binom{n}{0} \binom{n}{1} \binom{n}{2} \dots \binom{n}{n}$$

Ricordiamo che per $k=0$ e $k=n$ il coefficiente binomiale assume valore 1 (l'unico sottoinsieme di ordine 0 è l'insieme vuoto mentre l'unico sottoinsieme di ordine n è l'insieme stesso), e che, inoltre, vale la proprietà: $\binom{n}{k} = \binom{n}{n-k}$

Da questa proprietà segue che i valori dei coefficienti binomiali sono uguali “a coppie simmetriche”. Si possono distribuire i coefficienti binomiali in righe, una per ogni valore di n , e disporre in un triangolo, che prende il nome di **Triangolo di Tartaglia**:

$$\begin{array}{ccccccc} n=1 & & \binom{1}{0} & & \binom{1}{1} & & \\ n=2 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} \\ n=3 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ \dots & & \dots & & \dots & & \dots & & \dots \end{array}$$

Tartaglia notò che gli elementi di ogni riga sono legati a quelli della riga inferiore (successiva, cioè la riga con $n=n+1$); per esempio:

$$\binom{2}{1} = 2; \binom{2}{2} = 1 \text{ e } \binom{3}{2} = 3, \text{ cioè } \binom{3}{2} = \binom{2}{1} + \binom{2}{2} = 3$$

Si nota che ciò avviene sempre: la somma di 2 elementi consecutivi di una riga del triangolo di Tartaglia coincide con l'elemento della riga inferiore frapposto ad essi. Questo dipende dalla seguente regola generale:

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

Dimostriamo tale formula, utilizzando la seguente formula, già dimostrata, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Il secondo termine dell'uguaglianza che si vuole dimostrare è uguale a: $\frac{(n+1)!}{k!(n+1-k)!}$

mentre il primo termine è uguale a: $\frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!}$

Per calcolare il comune denominatore, si nota che $k! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot k = (k-1)! \cdot k$ ed allora:

$(n-k+1)! = 1 \cdot 2 \cdot \dots \cdot (n-k+1) = (n-k)! \cdot (n-k+1)$ da cui si ottiene:

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n! \cdot k + (n-k+1) \cdot n!}{k!(n-k+1)!} = \frac{n!(k + (n-k+1))}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!}$$

che è la tesi che si voleva dimostrare.

Tale formula permette di costruire “ricorsivamente” le righe del Triangolo di Tartaglia. I numeri estremi (cioè il primo e l'ultimo) sono uguali a 1 ($k=0$ e $k=n$), quelli intermedi si ottengono sommando a coppie gli elementi della riga superiore.

Esempio: se conosciamo la 3^a riga ($n=3$) possiamo ottenere la 4^a:

$$\begin{array}{ccccccc} \binom{3}{0}=1 & & \binom{3}{1}=3 & & \binom{3}{2}=3 & & \binom{3}{3}=1 \\ & \searrow & \swarrow & \searrow & \swarrow & \searrow & \swarrow \\ \binom{4}{0}=1 & & \binom{4}{1}=4 & & \binom{4}{2}=6 & & \binom{4}{3}=4 & & \binom{4}{4}=1 \end{array}$$

Dalla quarta si può quindi ottenere la quinta e così via.

Sviluppo della potenza di un binomio.

Ricordiamo il quadrato ed il cubo di un binomio:

$$(a+b)^2=a^2+2ab+b^2 \quad \text{e} \quad (a+b)^3=a^3+3a^2b+3ab^2+b^3$$

Si nota che i coefficienti dello sviluppo delle potenze di un binomio sono corrispondenti ai numeri di una riga del triangolo di Tartaglia:

2 ^a riga	$\binom{2}{0}=1, \binom{2}{1}=2, \binom{2}{2}=1$	$(a+b)^2=1*a^2+2ab+1*b^2$
3 ^a riga	$\binom{3}{0}=1, \binom{3}{1}=3, \binom{3}{2}=3, \binom{3}{3}=1$	$(a+b)^3=a^3+3a^2b+3ab^2+b^3$

In generale *sembra* valere la seguente formula che calcola la potenza di un binomio con esponente n qualunque (**sviluppo di Newton**):

$$(a+b)^n = \binom{n}{0} * a^{n-0}b^0 + \binom{n}{1} * a^{n-1}b^1 + \binom{n}{2} * a^{n-2}b^2 + \dots + \binom{n}{n} * a^0b^n$$

Dimostriamo la validità di tale formula per ogni esponente $n \geq 2$, ragionando per induzione.

Per $n=2$ si è già visto che la formula è valida; supponiamo allora che sia vera per un certo $n=k$, cioè che sia vero che:

$$(a+b)^k = \binom{k}{0} * a^{k-0}b^0 + \binom{k}{1} * a^{k-1}b^1 + \binom{k}{2} * a^{k-2}b^2 + \dots + \binom{k}{k} * a^0b^k$$

e cerchiamo di dimostrare che è valida anche per $n=k+1$, cioè che:

$$(a+b)^{k+1} = \binom{k+1}{0} * a^{k+1-0}b^0 + \binom{k+1}{1} * a^{k+1-1}b^1 + \binom{k+1}{2} * a^{k+1-2}b^2 + \dots + \binom{k+1}{k+1} * a^0b^{k+1}$$

Sappiamo che $(a+b)^{k+1}=(a+b)(a+b)^k$ quindi possiamo riscrivere l'uguaglianza da dimostrare nel modo seguente:

$$(a+b)^{k+1} = \left[\binom{k}{0} * a^{k-0}b^0 + \binom{k}{1} * a^{k-1}b^1 + \binom{k}{2} * a^{k-2}b^2 + \dots + \binom{k}{k} * a^0b^k \right] * (a+b)$$

Applicando la proprietà distributiva del prodotto:

$$(a+b)^{k+1} = \left(\binom{k}{0} a^{k-0} b^0 + \binom{k}{1} a^{k-1} b^1 + \dots + \binom{k}{k} a^0 b^k \right) a + \left(\binom{k}{0} a^{k-0} b^0 + \binom{k}{1} a^{k-1} b^1 + \dots + \binom{k}{k} a^0 b^k \right) b$$

Moltiplicando per a, si avrà un incremento di 1 dell'esponente di a mentre moltiplicando per b si avrà un incremento di 1 dell'esponente di b:

$$(a+b)^{k+1} = \left(\binom{k}{0} a^{k+1} b^0 + \binom{k}{1} a^k b^1 + \dots + \binom{k}{k} a^1 b^k \right) + \left(\binom{k}{0} a^{k-0} b^1 + \binom{k}{1} a^{k-1} b^2 + \dots + \binom{k}{k} a^0 b^{k+1} \right)$$

Associando i termini simili si ha:

$$(a+b)^{k+1} = \binom{k}{0} a^{k+1} b^0 + \left(\binom{k}{1} + \binom{k}{0} \right) a^k b^1 + \left(\binom{k}{2} + \binom{k}{1} \right) a^{k-1} b^2 + \dots$$

Osservando che, in base alla formula:

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

si ha che:

$$\binom{k}{0} = \binom{k+1}{0} = 1; \quad \binom{k}{1} + \binom{k}{0} = \binom{k+1}{1}; \quad \binom{k}{2} + \binom{k}{1} = \binom{k+1}{2}, \quad \text{etc.};$$

e si ottiene lo sviluppo di $(a+b)^{k+1}$ previsto, per cui vale il principio di induzione e la formula dello sviluppo di Newton è dimostrata.

Lezione n° 31 – 24 gen. 2001

Prodotto cartesiano di due insiemi.

Siano A e B due insiemi; una coppia con il primo elemento in A ed il secondo elemento in B è un oggetto della forma (a,b), con $a \in A$ e $b \in B$ (due coppie si considerano uguali se hanno uguali rispettivamente il primo elemento ed il secondo).

L'insieme di tutte le coppie possibili con il primo elemento in A ed il secondo in B è detto **prodotto cartesiano di A per B** ed è indicato con **$A \times B$** .

$$A \times B = \{z / z=(a,b) \text{ con } a \in A \text{ e } b \in B\}$$

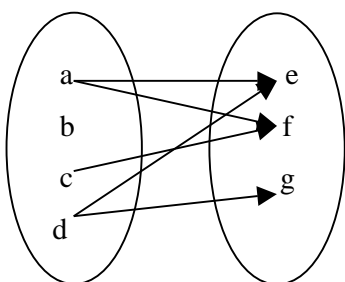
Se A e B sono insiemi finiti e se $|A|=n$ e $|B|=m$, le possibili coppie di $A \times B$ sono in numero di $n \cdot m$ (se gli elementi di A sono a_1, a_2, \dots, a_n e gli elementi di B sono b_1, b_2, \dots, b_m , le coppie che hanno come primo elemento a_1 sono m, quelle che hanno come primo elemento a_2 sono m e così via fino ad ottenere un numero totale di coppie pari a $m+m+\dots+m=m \cdot n$). Quindi $|A \times B| = |A| \cdot |B|$ (ricordare comunque che questo vale per insiemi finiti).

Esempio: siano $A=\{a,b,c\}$ e $B=\{1,2\}$, allora $A \times B = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$, cioè un totale di $|A| \cdot |B| = 3 \cdot 2 = 6$.

Se è data una relazione R dall'insieme A all'insieme B , si può costruire il sottoinsieme di $A \times B$ costituito dalle coppie il cui primo elemento è associato al secondo elemento dalla relazione R : $\{(a,b) \in A \times B / aRb\} \subseteq A \times B$.

Tale sottoinsieme è detto **insieme delle coppie della relazione R** .

Esempio: se $A=\{a,b,c,d\}$ e $B=\{e,f,g\}$ e se $R:A \rightarrow B$ è definita graficamente come segue:



l'insieme delle coppie della relazione R è:

$\{(a,e), (a,f), (b,f), (c,f), (d,e), (d,g)\}$;

sono in totale 5 coppie sulle 12 in totale di $A \times B$.

Contare le coppie di una relazione “per righe e per colonne”.

Se A e B sono due insiemi finiti e se $|A|=n$ e $|B|=m$ e se esiste la relazione $R:A \rightarrow B$, la R si può rappresentare in forma matriciale con una matrice con n righe (corrispondenti agli elementi di A) ed m colonne (corrispondenti agli elementi di B):

$A \downarrow B \rightarrow$	b_1	b_2	b_m
a_1							
a_2							
...							
...							
a_n							

Nella generica casella vi è un 1 se l'elemento della riga è associato a quello della colonna, uno zero se invece non lo è.

Ovviamente il numero di 1 nella matrice corrisponde al numero di coppie della relazione R .

Tale numero di 1 si può contare in due modi diversi:

1. contare gli 1 presenti in ogni riga e sommare i risultati;
2. contare gli 1 presenti in ogni colonna e sommare i risultati.

Ovviamente il risultato deve essere lo stesso. Questo porta spesso delle informazioni su alcuni tipi di problemi (quelli in cui il problema si riconduce alla costruzione di una relazione fra due insiemi finiti).

Esempio 1: siano dati n studenti, ognuno dei quali sceglie 4 corsi da seguire su 7 in totale. È possibile che le iscrizioni ai corsi siano le seguenti?

1° corso: 52 studenti; 2° corso: 30 studenti; 3° corso: 30 studenti; 4° corso: 20 studenti;
5° corso: 25 studenti; 6° corso: 12 studenti; 7° corso: 18 studenti.

Svolgimento: se A è l'insieme degli n studenti e B quello dei 7 corsi, si può costruire una relazione $R:A \rightarrow B$ associando ad ogni studente i 4 corsi a cui è iscritto; la matrice della relazione è del tipo:

A \ B	1	2	3	4	5	6	7
1							
2							
....							
....							
n							

Possiamo contare gli 1 presenti in due modi:

1. per righe ed in totale avremo un numero di 1 pari a $4 \cdot n$;
2. per colonne ed avremo un totale pari alla somma degli studenti iscritti ai 7 corsi che sono: $52+30+30+20+25+12+18=187$.

Poiché i due *conteggi* devono coincidere, deve essere $4 \cdot n = 187$, ma ciò non è possibile perché 187 non è un multiplo di 4, per cui ci sarà sicuramente un errore nei dati forniti sulle iscrizioni ai corsi.

Esempio 2: in una classe ci sono n studenti, dei quali 32 ragazzi. Ogni ragazzo conosce 5 ragazze e ogni ragazza conosce 8 ragazzi. Quanti studenti ci sono in tutto nella classe?

Svolgimento: se A è l'insieme dei ragazzi e B quello delle ragazze possiamo definire una relazione $R:A \rightarrow B$ di "conoscenza"; la matrice corrispondente avrà 32 righe ed x colonne (dove x è il numero delle ragazze). Se contiamo gli 1 per righe avremo un totale di $32 \cdot 5 = 160$, contandoli per colonne avremo un totale di $8 \cdot x$. Poiché i due totali devono coincidere possiamo scrivere l'equazione in x : $8x = 160$ dalla quale ricaviamo il numero delle ragazze che è 20. Allora in totale nella classe ci saranno $32+20=52$ studenti.

Esercizio: dato un insieme A con 8 elementi, è possibile trovare dei sottoinsiemi di A tali che ognuno di essi abbia 3 elementi e tali che ogni elemento di A appartenga esattamente a 5 di questi sottoinsiemi?

Svolgimento: sia X l'insieme dei sottoinsiemi di A contenenti 3 elementi; definiamo una relazione da A in X associando degli elementi di A ai sottoinsiemi che li contengono. Per le condizioni poste, in ogni colonna dovranno esserci 3 valori 1 ed in ogni riga 5 valori 1. Contando per righe il numero totale di 1 sarà $8 \cdot 5 = 40$, contando per colonne il numero di 1 sarà $n \cdot 3$ (dove n è il numero di sottoinsiemi di A contenenti 3 elementi e tali che ogni elemento di A appartenga esattamente a 5 di essi). Allora, visto che i due conteggi devono coincidere si può scrivere l'equazione nell'incognita n : $n \cdot 3 = 40$ dalla quale, non essendo 40

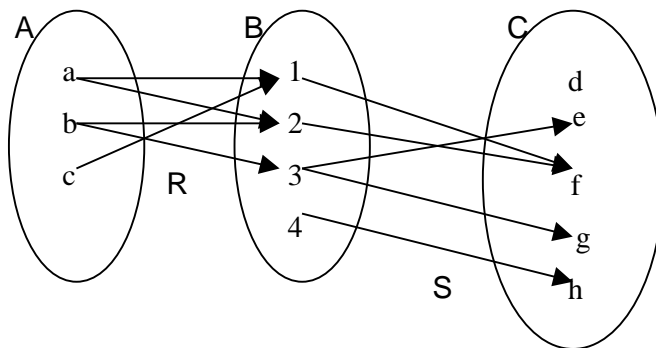
divisibile per 3, si evince che non è possibile ottenere dei sottoinsiemi di ordine 3 e tali che ogni elemento di A sia contenuto esattamente in 5 di essi.

Lezione n° 32 – 26 gen. 2001

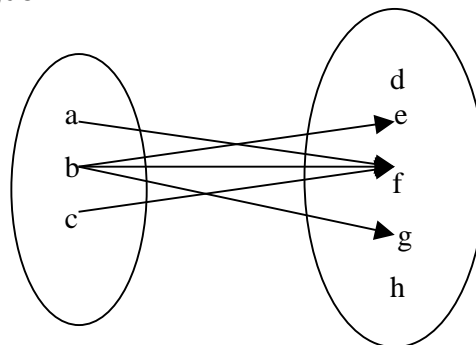
In riferimento all'esercizio precedente: notare che, se i dati fossero stati gli stessi ma con la condizione che ogni elemento comparisse in 6 sottoinsiemi (e non 5), si sarebbe giunti ad una equazione in n $48=3*n$ che trova soluzione per $n=16$, per cui sarebbe stato possibile costruire dei sottoinsiemi di ordine 3 con la condizione richiesta; il ragionamento seguito fornisce anche il numero di questi sottoinsiemi. Però, chi assicura che i 16 sottoinsiemi si possano effettivamente costruire? La risposta a questo interrogativo sarà data dalla "Teoria dei disegni" che si studierà in seguito.

Composizione di relazioni.

Siano dati 3 insiemi A, B, C, ad esempio $A=\{a,b,c\}$, $B=\{1,2,3,4\}$ e $C=\{d,e,f,g,h\}$ e data una relazione R da A a B ed una relazione S da B a C, ad esempio, graficamente:



Si può costruire una nuova relazione T da A a C (dove B funziona da "ponte di passaggio"), come segue:



In pratica, dato un elemento $x \in A$ ed un elemento $y \in C$, si ha xTy quando esiste almeno un elemento $z \in B$ tale che xRz e zSy .

Tale nuova relazione T è detta **composizione di R ed S** ed è indicata con il simbolo $S \circ R$. (Notare che la relazione R è scritta *dopo*, nel simbolo).

Composizioni di applicazioni.

Se, in particolare, sono dati tre insiemi A , B , e C e due *applicazioni* $f: A \rightarrow B$ e $g: B \rightarrow C$, si può definire la relazione composta $g \circ f$. Nella relazione composta, un elemento $x \in A$ è associato ad un elemento $y \in C$, quando esiste almeno un elemento $z \in B$ tale che $f(x)=z$ e $g(z)=y$. È ovvio che di tali z ve ne è uno solo, perché f è un'applicazione, così come anche y è unico perché anche g è un'applicazione. In conclusione, la composizione di due applicazioni è ancora un'applicazione.

Vediamo come *agisce* formalmente la composizione $g \circ f$ cioè cerchiamo di capire, dato un elemento $x \in A$, qual è il suo corrispondente in C .

Per costruzione, si ha che $(g \circ f)(x)=g(f(x))$, infatti prima si calcola il corrispondente in B di x mediante f e poi, del risultato, si calcola il corrispondente in C mediante g .

Se f e g sono definite da formule, per calcolare la formula che definisce la composizione $g \circ f$ si opera "per sostituzione": per esempio, se $A=\mathbb{Z}$, $B=\mathbb{Q}$ e $C=\mathbb{R}$ e se sono date le applicazioni $f: \mathbb{Z} \rightarrow \mathbb{Q}$ e $g: \mathbb{Q} \rightarrow \mathbb{R}$ con le formule seguenti:

$$f(x)=(x-2)/3 \quad \text{e} \quad g(x)=+\sqrt{x^2+7}$$

la composizione $(g \circ f): \mathbb{Z} \rightarrow \mathbb{R}$ sarà definita dalla formula:

$$(g \circ f)(x)=g(f(x))=g((x-2)/3)=+\sqrt{\left(\frac{x-2}{3}\right)^2+7}$$

Se $f: A \rightarrow B$ e $g: B \rightarrow C$ sono entrambe applicazioni iniettive, allora anche la composizione $g \circ f$ è un'applicazione iniettiva; infatti, presi due elementi distinti di A , $a_1, a_2 \in A$ si ha che $f(a_1), f(a_2) \in B$ sono anch'essi distinti (per l'iniettività dell'applicazione f) e quindi anche gli elementi $g(f(a_1)), g(f(a_2)) \in C$ saranno distinti (per l'iniettività dell'applicazione g).

Esercizi:

1. *dimostrare che la composizione di due applicazioni surgettive è ancora surgettiva.*
2. *se $g \circ f$ è iniettiva, si può affermare con certezza che f e g sono entrambe iniettive?
E se $g \circ f$ è surgettiva, si può affermare che f e g sono entrambe surgettive?*

Svolgimento 1: perché la composizione di g e f sia surgettiva deve succedere che, comunque preso $y \in C$ esiste sempre un elemento x in A tale $y=g(f(x))$; la surgettività di g ci assicura che, per ogni $y \in C$ esiste sempre un elemento $z \in B$ tale che $y=g(z)$ e la

surgettività di f ci assicura che, per ogni $z \in B$ esiste sempre un elemento $x \in A$ tale che $z=f(x)$ e quindi che, per ogni $y \in C$ esiste sempre un elemento x in A tale $y=g(f(x))$.

Svolgimento 2: l'iniettività di $g \circ f$ implica che, comunque presi $x_1, x_2 \in A$, $g(f(x_1)), g(f(x_2)) \in C$ sono anch'essi elementi distinti. Ora, $f(x_1) \neq f(x_2)$ in B perché se così non fosse, si avrebbe un elemento di B con una doppia immagine in C e ciò va contro la definizione stessa di applicazione, quindi la f è un'applicazione iniettiva. Riguardo all'applicazione g non si può dire nulla, perché potrebbe esistere un elemento $z \in B$ tale che, ad esempio, $g(z)=y_1$ e tale che z non sia l'immagine tramite la f di nessun elemento di A .

Se invece $g \circ f$ è surgettiva, ciò implica che, comunque preso $y \in C$ esiste sempre $x \in A$ tale che $g(f(x))=y$. Questo implica anche che per ogni $y \in C$ esiste sempre un elemento "di passaggio" $z \in B$, tale che $g(z)=y$, quindi che l'applicazione g è surgettiva. Nulla si può invece dire riguardo l'applicazione f , perché potrebbe esistere in B un elemento z che non sia l'immagine di alcun elemento di A tramite la f .

Lezione n°. 33 – 31 gen. 2001

Correzione esercizi lasciati per casa.

Lezione n°. 34 – 2 feb. 2001

Se A , B e C sono tre insiemi finiti, rispettivamente di ordine n , m , k e se sono date due relazioni R da A a B ed S da B a C , rappresentando queste ultime con matrici si ottengono una matrice con n righe ed m colonne per la relazione R ed una matrice con m righe e k colonne per la relazione S . Si può costruire la relazione composta $S \circ R$ da A a C e la si può rappresentare con una terza matrice, che avrà n righe e k colonne. Come si ottiene tale matrice dalle matrici delle due relazioni R ed S ? Per dare una risposta a questa domanda si devono introdurre due nuovi concetti: il **prodotto di matrici** ed il **prodotto booleano**.

Prodotto di matrici.

Siano date due matrici M_1 ed M_2 , la prima con n righe ed m colonne e la seconda con m righe e k colonne (il numero di righe della seconda coincide con il numero di colonne della prima). Supponiamo che nelle caselle di tali matrici vi siano dei numeri generici (cioè non necessariamente 0 ed 1), e proviamo a costruire una terza matrice M_3 , detta **prodotto**

righe per colonne delle due matrici date. Definiamo il significato di prodotto di una riga della prima matrice per una colonna della seconda:

M_1	m colonne								
n									
r									
i									
g									
h									
e									

M_2	k colonne								
m									
r									
i									
g									
h									
e									

Sia la generica riga della prima matrice che la generica colonna della seconda contengono esattamente m numeri. Si definisce **prodotto** di tale riga e di tale colonna quel numero ottenuto moltiplicando ordinatamente (cioè quelli con indici corrispondenti) i numeri della riga per quelli della colonna e sommando i risultati di tali moltiplicazioni.

Esempio:

-1	2	3	-5	

	2			
	0			
	3			
	-1			

Il prodotto della riga scelta per la colonna scelta è:
 $(-1)*2+2*0+3*3+(-5)*(-1)=12$

Definiamo adesso il **prodotto righe per colonne di due matrici**: è una terza matrice, di n righe e k colonne, nella quale, in ogni casella si inserisce un numero determinato con la seguente regola: se la casella si trova all'incrocio tra la riga di indice r e la colonna di indice s, il numero da essa contenuto è dato dal prodotto della riga r della matrice M_1 per la colonna s della matrice M_2 .

Esempio:

1	0	-2	3
1	2	1	4
0	2	5	-3

0	1
2	7
-1	0
0	1

Il prodotto righe per colonne di queste due matrici sarà una matrice con 3 righe e 2 colonne. Il contenuto delle 6 caselle è determinato secondo la regola enunciata; partendo dalla casella in alto a sinistra e procedendo in senso orario, avremo;

$$1*0+0*2+(-2)*(-1)+3*0=2$$

$$1*1+0*7+(-2)*0+3*1=4$$

$$1*1+2*7+1*0+4*1=19$$

$$0*1+2*7+5*0+(-3)*1=11$$

$$0*0+2*2+5*(-1)+(-3)*0=-1$$

$$1*0+2*2+1*(-1)+4*0=3$$

2	4
3	19
-1	11

Prodotto booleano di matrici.

Siano date due matrici M_1 ed M_2 , la prima con n righe ed m colonne e la seconda con m righe e k colonne (il numero di righe della seconda coincide con il numero di colonne della prima). Supponiamo che nelle caselle di tali matrici vi siano solo numeri 0 o 1. Il loro prodotto booleano è una terza matrice M_3 di n righe e k colonne contenente nelle caselle solo numeri 0 o 1, determinati con il prodotto righe per colonne già visto ma con la seguente regola aritmetica particolare per la somma:

$0+0=0$, $0+1=1+0=1$, $1+1=1$.

Notare che tale regola corrisponde alla tavola di verità della disgiunzione logica (OR).

Notare ancora che, nella somma booleana ora definita, se sono presenti diversi addendi, la loro somma è 0 se sono tutti uguali a 0 mentre è 1 se almeno uno di essi è uguale a 1.

Teorema: se A , B e C sono tre insiemi finiti, rispettivamente di ordine n , m , k e se sono date due relazioni R da A a B ed S da B a C , rappresentate rispettivamente dalle matrici M_1 (di n righe ed m colonne) ed M_2 (di m righe e k colonne), allora la matrice della relazione composta $S \circ R$ da A a C coincide con il prodotto booleano delle due matrici M_1 ed M_2 .

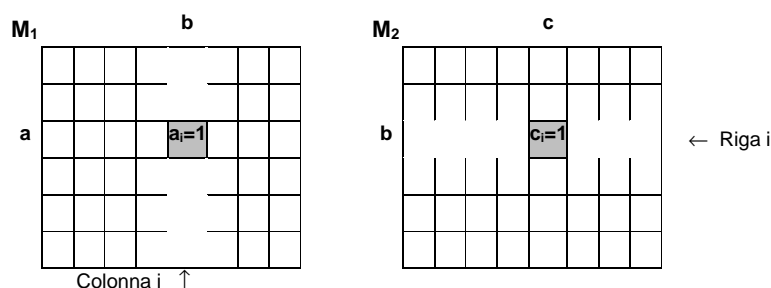
Dimostrazione: si consideri il prodotto booleano M_3 delle due matrici M_1 ed M_2 ; la tesi è che M_3 sia la matrice della relazione $S \circ R$ e cioè che, dato un elemento $a \in A$ ed un elemento $c \in C$ (con a che corrisponde ad una riga della matrice M_1 e c che corrisponde ad una colonna della matrice M_2 , deve verificarsi che all'incrocio fra la riga a e la colonna c della matrice M_3 vi sia un valore 1 se a è associato a c tramite $S \circ R$ ed un valore 0 in caso contrario. Nella casella posta all'incrocio tra la riga a e la colonna c della matrice M_3 si pone, per costruzione, il prodotto booleano della riga a della matrice M_1 per la colonna c della matrice M_2 :

M_1		M_2	c	M_3	c
a					

Ma se la riga a e la colonna c sono come segue:

$$\begin{array}{c|cccc} a_1 & a_2 & \dots & \dots & a_m \end{array} \quad \begin{array}{c} \hline c_1 \\ c_2 \\ \dots \\ \dots \\ c_m \\ \hline \end{array}$$

con i numeri a_1, a_2, \dots, a_m e c_1, c_2, \dots, c_m che sono 0 o 1, operando il prodotto della riga per la colonna, si ottiene il numero $a_1 * c_1 + a_2 * c_2 + \dots + a_m * c_m$ (con la somma booleana). Tale somma darà risultato uguale a 1 solo nel caso in cui almeno un addendo è uguale a 1, cioè solo quando almeno un prodotto $a_i * c_i = 1$, cioè $a_i = c_i = 1$, cioè quando:



Quindi l'elemento $a \in A$ è in relazione tramite R con l'elemento $b \in B$ nella colonna i di M_1 e l'elemento $c \in C$ è in relazione tramite S con l'elemento $b \in B$ nella riga i di M_2 (b è lo stesso elemento, quello che fa da "ponte di passaggio"): ciò equivale a dire che a è in relazione con c tramite la relazione composta $S \circ R$, che è quanto si voleva dimostrare.

Esercizio: dati gli insiemi $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3, b_4\}$ e $C = \{c_1, c_2, c_3\}$ e le relazioni R da A a B ed S da B a C definite dalle due matrici seguenti:

R	b_1	b_2	b_3	b_4
a_1	1	1	0	0
a_2	0	1	1	0
a_3	0	0	0	1

S	c_1	c_2	c_3
b_1	1	0	0
b_2	1	0	0
b_3	1	0	0
b_4	0	0	1

Calcolare la matrice della relazione $S \circ R$ e verificare, sulla matrice, se essa è una applicazione da A a C .

Svolgimento: la matrice rappresentativa della relazione composta $S \circ R$ sarà una matrice con 3 righe e 3 colonne. Calcolo i valori delle diverse caselle operando i prodotti righe per colonne.

$S \circ R$	c_1	c_2	c_3
a_1	1	0	0
a_2	1	0	0
a_3	0	0	1

La relazione composta $S \circ R$ è un'applicazione da A in C poiché sulla sua matrice c'è un solo valore 1 per ogni riga.

Lezione n°. 35 – 5 feb. 2001

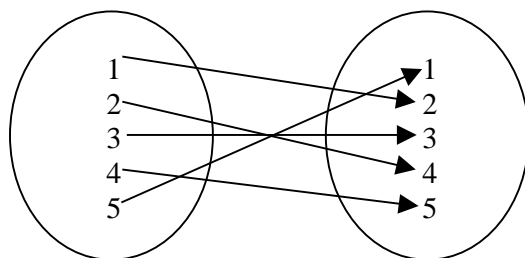
L'insieme S_n .

Fissato un intero $n > 1$, consideriamo l'insieme $\{1, 2, 3, 4, \dots, n\}$ dei primi n numeri naturali; se $f: \{1, 2, 3, 4, \dots, n\} \rightarrow \{1, 2, 3, 4, \dots, n\}$ è un'applicazione biunivoca, useremo il seguente simbolo per indicare l'applicazione f :

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

(nella prima riga vi sono i numeri $1, 2, \dots, n$, nel loro ordine naturale, nella seconda riga vi sono le rispettive immagini tramite l'applicazione f).

Esempio: se $n=5$ ed $f: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$ è definita graficamente da



allora si usa il simbolo $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

Indicheremo con il simbolo S_n l'insieme di tutte le applicazioni biunivoche da $\{1, 2, 3, 4, \dots, n\}$ in $\{1, 2, 3, 4, \dots, n\}$.

Sappiamo che il numero di elementi di S_n è $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$.

Esempio:

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} \quad \text{cioè } 2! = 1 \cdot 2 = 2$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \quad \text{cioè } 3! = 1 \cdot 2 \cdot 3 = 6$$

Per $n=4$ si avrà $4! = 24$ etc.

Notare che in S_n vi è sempre l'applicazione identica (che associa ad ogni elemento di $\{1, 2, 3, 4, \dots, n\}$ l'elemento stesso). Inoltre, data un'applicazione f in S_n , si può sempre costruire la sua inversa $f^{-1} \in S_n$.

Esempio: se

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 2 & 1 \end{pmatrix} \in S_6$$

Allora la f associa 1 a 3, 2 a 6, 3 a 5, 4 a 4, 5 a 2 e 6 a 1. La f^{-1} assocerà 3 a 1, 6 a 2, 5 a 3, 4 a 4, 2 a 5 e 1 a 6, per cui si potrà scrivere:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 3 & 2 \end{pmatrix} \in S_6$$

Se sono dati due elementi $f, g \in S_n$ dove f e g sono due applicazioni biunivoche da $\{1, 2, 3, 4, \dots, n\}$ in $\{1, 2, 3, 4, \dots, n\}$, si possono costruire le applicazioni composizione:

- $f \circ g: \{1, 2, 3, 4, \dots, n\} \rightarrow \{1, 2, 3, 4, \dots, n\}$ (in cui prima si applica la g e poi la f al risultato);
- $g \circ f: \{1, 2, 3, 4, \dots, n\} \rightarrow \{1, 2, 3, 4, \dots, n\}$ (in cui prima si applica la f e poi la g al risultato).

Poiché la composizione di applicazioni biunivoche è ancora un'applicazione biunivoca, si avrà che $f \circ g \in S_n$ e che $g \circ f \in S_n$.

In generale le due composizioni sono applicazioni diverse.

Esempio: siano date le due applicazioni

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Si otterranno le due applicazioni composizione seguenti:

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix} \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

Notiamo adesso che, scrivendo gli elementi di S_n con la simbologia

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

la seconda riga corrisponde ad una disposizione semplice degli n numeri $\{1, 2, \dots, n\}$ presi ad n ad n , cioè alle cosiddette **permutazioni** dei numeri $\{1, 2, \dots, n\}$. Per estensione di linguaggio chiameremo **permutazioni** anche gli elementi di S_n .

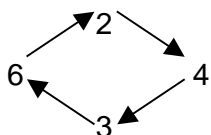
Permutazioni cicliche.

Sia data una permutazione $f \in S_n$; tale f è detta **permutazione ciclica** (o, più semplicemente **ciclo**) se la f *muove ciclicamente* alcuni dei numeri $1, 2, \dots, n$ lasciando *fermi* gli (eventuali) altri (nel senso che potrebbe anche muoverli tutti).

Esempio:

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 3 & 5 & 2 & 7 \end{pmatrix} \in S_7$ è una permutazione ciclica perché la sua azione è la seguente: muove ciclicamente 2, 4, 3, 6 (nel senso che 2 va in 4, 4 va in 3, 3 va in 6 e 6 va in 2) e lascia fermi gli altri numeri 1, 5, 7.

Schematicamente:



Si definisce **lunghezza di un ciclo f** il numero di interi fra 1 ed n che f muove ciclicamente (nell'esempio fatto il ciclo f ha lunghezza 4).

La permutazione identica (che lascia fermi tutti i numeri fra 1 ed n) si considera (per convenzione) anch'essa un ciclo, di lunghezza uguale a zero.

Per i cicli si userà una simbologia particolare: se $f \in S_n$ è un ciclo e se f muove ciclicamente i numeri i_1, i_2, \dots, i_k (nel senso che $i_1 \rightarrow i_2, i_2 \rightarrow i_3, \dots, i_{k-1} \rightarrow i_k, i_k \rightarrow i_1$) si scriverà $f = (i_1 i_2 \dots i_k)$, (in pratica si scrivono, nell'ordine in cui avvengono i *passaggi*, solo i numeri coinvolti, senza scrivere quelli che rimangono fermi).

Riferendosi all'esempio precedente, si scriverà $f = (2 4 3 6) \in S_7$.

Si noti che il simbolo non è univoco, nel senso che, facendo "scivolare" gli elementi del simbolo, il ciclo non cambia:

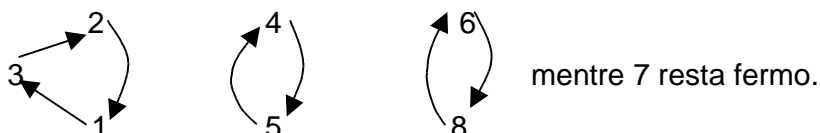
$$f = (2 4 3 6) = (6 2 4 3) = (3 6 2 4) = (4 3 6 2).$$

Non tutti gli elementi di S_n sono cicli.

Esempio:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 5 & 4 & 8 & 7 & 6 \end{pmatrix} \in S_8$$

Non è un ciclo perché la sua azione è la seguente:



Si dimostrerà che, anche se f non è un ciclo, in ogni caso si può ottenere come **composizione di cicli**.

Lezione n°. 36 – 7 feb. 2001

Esiste il seguente teorema (del quale si ometterà la dimostrazione):

teorema: ogni permutazione $f \in S_n$ è composizione di cicli (per composizione di cicli si intende, al limite, anche di cicli con un solo elemento).

Da un punto di vista *operativo* si procede come nell'esempio seguente:

esempio:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 5 & 6 & 1 & 4 & 8 & 7 & 9 \end{pmatrix} \in S_9$$

Osserviamo graficamente l'azione della f:

2 e 9 vengono lasciati fermi. La f si decompone nella applicazione di 3 cicli.

Trasposizione.

Una **trasposizione** in S_n è un ciclo di lunghezza 2 del tipo $f=(a\ b)$ (in pratica f scambia tra loro i numeri a e b , lasciando fermi gli altri).

Esempio:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix} \in S_6$$

$f=(1\ 5)=(5\ 1)$ è una trasposizione.

I cicli sono “mattoni” con i quali si costruiscono, per composizione, tutte le permutazioni di S_n ; le trasposizioni si possono allora interpretare come “mattoni elementari” perché sussiste il seguente teorema:

Teorema: ogni permutazione di S_n si può decomporre in composizione di trasposizioni.

Dimostrazione: per il teorema precedente, basta dimostrare che ogni ciclo è composizione di trasposizioni. Sia allora dato un ciclo qualunque $f \in S_n$ (un caso particolare è la permutazione identica: essa si può decomporre in composizione di trasposizioni, ad esempio: $(1\ 2)^o(2\ 1) =$ permutazione identica, perché 1 va in 2 nella prima trasposizione e poi torna nuovamente a 1 nella seconda). Se $f \in S_n$ è quindi un ciclo diverso dalla permutazione identica e se la sua lunghezza è k , si avrà: $f=(i_1\ i_2\ \dots\ i_k)$; per avere la tesi (che f è composizione di trasposizioni) dobbiamo dimostrare che

$$f=(i_1\ i_2\ \dots\ i_k)=(i_1\ i_k)^o(i_1\ i_{k-1})^o(i_1\ i_{k-2})^o\dots\dots^o(i_1\ i_3)^o(i_1\ i_2).$$

Per dimostrare che due permutazioni sono uguali, si deve verificare che, prendendo un qualunque numero intero h compreso tra 1 ed n l'azione delle due permutazioni sul numero h sia la stessa. Le permutazioni in questione sono il ciclo $f=(i_1\ i_2\ \dots\ i_k)$ e la composizione $(i_1\ i_k)^o(i_1\ i_{k-1})^o(i_1\ i_{k-2})^o\dots\dots^o(i_1\ i_3)^o(i_1\ i_2)$. Sia allora h un numero intero compreso fra 1 ed n . Distinguiamo tre casi:

1. h è diverso dai numeri i_1, i_2, \dots, i_k .

l'azione di f su h è $h \rightarrow h$ (infatti se h non compare nel ciclo vuol dire che rimane fermo),

l'azione di $(i_1\ i_k)^o(i_1\ i_{k-1})^o\dots\dots^o(i_1\ i_3)^o(i_1\ i_2)$ è:

$(i_1\ i_2)$	$(i_1\ i_3)$	$(i_1\ i_{k-1})$	$(i_1\ i_k)$
$h \rightarrow h$	$h \rightarrow h$	$h \rightarrow h$	$h \rightarrow h$

(Ricordare che le permutazioni composte si applicano da destra verso sinistra).

L'azione delle due permutazioni coincidono, infatti nessuna delle due *muove* h .

2. h è uno dei numeri i_1, i_2, \dots, i_k .

1° sottocaso: $h=i_1$.

L'azione di f è $h=i_1 \rightarrow i_2$ infatti il ciclo è $f=(i_1 i_2 \dots i_k)$.

L'azione di $(i_1 i_k)^o (i_1 i_{k-1})^o \dots (i_1 i_3)^o (i_1 i_2)$ è:

$(i_1 i_2)$	$(i_1 i_3)$	$(i_1 i_{k-1})$	$(i_1 i_k)$
$h=i_1 \rightarrow i_2$	$i_2 \rightarrow i_2$	$i_2 \rightarrow i_2$	$i_2 \rightarrow i_2$

Dopo la prima permutazione, i_2 non compare più nelle successive permutazioni, quindi anche in questo caso l'azione delle due permutazioni in questione è la stessa.

2° sottocaso: $h=i_2$.

L'azione di f è $h=i_2 \rightarrow i_3$ infatti il ciclo è $f=(i_1 i_2 \dots i_k)$.

L'azione di $(i_1 i_k)^o (i_1 i_{k-1})^o \dots (i_1 i_3)^o (i_1 i_2)$ è:

$(i_1 i_2)$	$(i_1 i_3)$	$(i_1 i_{k-1})$	$(i_1 i_k)$
$h=i_2 \rightarrow i_1$	$i_1 \rightarrow i_3$	$i_3 \rightarrow i_3$	$i_3 \rightarrow i_3$

Dopo la seconda permutazione, i_3 non compare più nelle successive permutazioni, quindi anche in questo caso l'azione delle due permutazioni in questione è la stessa.

Questo ragionamento vale anche per tutti gli altri *sottocasi* (valori di h fino ad $n-1$).

3. $h=i_k$.

L'azione di f è: $h=i_k \rightarrow i_1$ infatti il ciclo è $f=(i_1 i_2 \dots i_k)$.

L'azione di $(i_1 i_k)^o (i_1 i_{k-1})^o \dots (i_1 i_3)^o (i_1 i_2)$ è:

$(i_1 i_2)$	$(i_1 i_3)$	$(i_1 i_{k-1})$	$(i_1 i_k)$
$h=i_k \rightarrow i_k$	$i_k \rightarrow i_k$	$i_k \rightarrow i_k$	$i_k \rightarrow i_1$

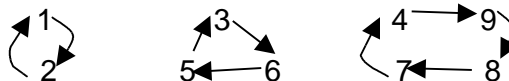
$h=i_k$ non compare fino alla penultima permutazione, quindi non varia, mentre all'ultima va in i_1 .

Anche in questo caso allora le due trasposizioni hanno su h la stessa azione.

Si è verificato che, per qualsiasi valore di h tra 1 ed n le due permutazioni hanno la stessa azione su h e quindi il teorema è dimostrato.

Esempio:

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 6 & 9 & 3 & 5 & 4 & 7 & 8 \end{pmatrix} \in S_9$ Prima decomponiamo in cicli:



allora $f=(1 \ 2)^o (3 \ 6 \ 5)^o (4 \ 9 \ 8 \ 7)$. Adesso decomponiamo i cicli in trasposizioni, seguendo il metodo visto nella dimostrazione del teorema.

$(1 \ 2)$ è già una trasposizione, $(3 \ 6 \ 5)=(3 \ 5)^o (3 \ 6)$ e $(4 \ 9 \ 8 \ 7)=(4 \ 7)^o (4 \ 8)^o (4 \ 9)$, quindi, infine:
 $f=(1 \ 2)^o (3 \ 5)^o (3 \ 6)^o (4 \ 7)^o (4 \ 8)^o (4 \ 9)$.

Esercizio: date le permutazioni in S_8 :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 5 & 7 & 6 & 8 & 2 \end{pmatrix} \in S_8 \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 4 & 6 & 8 & 3 & 7 \end{pmatrix} \in S_8$$

Scomporre in trasposizioni f^{-1} , g^{-1} , $f^o g$ e $g^o f$.

Svolgimento: trovo intanto le espressioni di f^{-1} , g^{-1} , $f^o g$ e $g^o f$.

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 1 & 2 & 4 & 6 & 5 & 7 \end{pmatrix} \in S_8 \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 4 & 3 & 5 & 8 & 6 \end{pmatrix} \in S_8$$

$$f^o g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 6 & 2 & 1 & 8 \end{pmatrix} \in S_8 \quad g^o f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 6 & 3 & 8 & 7 & 2 \end{pmatrix} \in S_8$$

Adesso individuo i cicli di ogni permutazione e poi, in base al teorema sulla scomposizione dei cicli in trasposizioni, scompongo in trasposizioni:

$$f^{-1} = (1 \ 3)^o (2 \ 8 \ 7 \ 5 \ 4) = (1 \ 3)^o (2 \ 4)^o (2 \ 5)^o (2 \ 7)^o (2 \ 8)$$

$$g^{-1} = (3 \ 7 \ 8 \ 6 \ 5) = (3 \ 5)^o (3 \ 6)^o (3 \ 8)^o (3 \ 7)$$

$$f^o g = (1 \ 3 \ 7)^o (2 \ 4 \ 5 \ 6) = (1 \ 7)^o (1 \ 3)^o (2 \ 6)^o (2 \ 5)^o (2 \ 4)$$

$$g^o f = (1 \ 5 \ 3)^o (2 \ 4 \ 6 \ 8) = (1 \ 3)^o (1 \ 5)^o (2 \ 8)^o (2 \ 6)^o (2 \ 4)$$

Lezione n°. 37 – 9 feb. 2001

Osservazioni:

1. se $f \in S_n$ e se $i \in S_n$ è la permutazione identica, cosa si può dire sulle composizioni $f^o i$ e $i^o f$?

Per un generico numero intero $x \in \{1, 2, \dots, n\}$ si ha che $x \rightarrow x$ tramite la i e poi $x \rightarrow y$ tramite la f , oppure che $x \rightarrow y$ tramite la f e poi $y \rightarrow y$ tramite la i . In pratica si nota che $i^o f$ ed $f^o i$ hanno lo stesso effetto di f sul generico x , quindi $i^o f = f^o i = f$.

La permutazione identica si può considerare elemento *neutro* rispetto alla composizione.

2. se $f \in S_n$ e se si considera $f^{-1} \in S_n$, cosa si può dire sulle composizioni $f^o f^{-1}$ e $f^{-1} o f$?

Per un generico numero intero $x \in \{1, 2, \dots, n\}$ si ha che $x \rightarrow y$ tramite la f e poi $y \rightarrow x$ tramite la f^{-1} nel primo caso, oppure che $x \rightarrow z$ tramite la f^{-1} e poi $z \rightarrow x$ tramite la f nel secondo caso. In pratica si nota che $f^o f^{-1}$ e $f^{-1} o f$ coincidono con la permutazione identica, quindi: $f^o f^{-1} = f^{-1} o f = i$.

Permutazioni di classe pari e di classe dispari.

Sia data una $f \in S_n$,

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

dove $1 \rightarrow i_1, 2 \rightarrow i_2, 3 \rightarrow i_3, \dots, n \rightarrow i_n$.

Presi due numeri nella seconda riga, i_r ed i_s , (sono sempre interi compresi tra 1 ed n), si dirà che f presenta una **inversione in i_r, i_s** se i_r ed i_s sono, nella seconda riga, in ordine inverso rispetto a quello naturale (cioè si trova a sinistra quello maggiore).

Esempio:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in S_5$$

f presenta le inversioni in 2-1, in 3-1, in 4-1, in 5-1. Non presenta inversione, ad esempio, in 3-4.

Si dirà che **f è di classe pari** (o, più in breve, **pari**), se il numero di inversioni che essa presenta è pari, altrimenti si dirà **di classe dispari** (o solo **dispari**). Nell'esempio precedente la f è di classe pari (sono in tutto 4 inversioni). Ovviamente la permutazione identica non presenta alcuna inversione: per convenzione (poiché si può scrivere $0=2*0$, cioè come multiplo di due), essa si considera di classe pari.

Esiste un algoritmo che permette di stabilire molto velocemente se una permutazione è pari o dispari.

Prima bisogna introdurre il seguente lemma:

lemma: se $f \in S_n$ e se è data una trasposizione $(a\ b) \in S_n$, si ha che la composizione $(a\ b)^o f$ ha una *parità* diversa da quella di f (cioè: se f è pari allora $(a\ b)^o f$ è dispari e viceversa)

dimostrazione:

sia data la permutazione:

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

Poiché i numeri a e b sono compresi tra 1 ed n , compariranno in qualche posizione nella seconda riga di f , cioè:

$$f = \begin{pmatrix} 1 & 2 & \dots & a & \dots & b & \dots & n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Calcoliamo adesso la composizione:

$$(a\ b)^o f = \begin{pmatrix} 1 & 2 & \dots & b & \dots & a & \dots & n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

In pratica, in $(a\ b)^o f$, la seconda riga è immutata, tranne per i numeri a e b che si scambiano.

Dimostriamo la tesi del lemma distinguendo 2 casi:

1° caso: a e b sono adiacenti nella seconda riga di f, cioè:

$$f = \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & \dots & i_k & a & b & j_1 & \dots & \dots & j_r \end{pmatrix}$$

La composizione sarà:

$$(a \ b)^{\circ} f = \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & \dots & i_k & b & a & j_1 & \dots & \dots & j_r \end{pmatrix}$$

si nota che la situazione del numero di inversioni nei due casi è la stessa tranne che per i due numeri a e b: lo scambio di a e b fa nascere una nuova inversione nel caso in cui in f erano nel loro ordine naturale, o la fa sparire se invece non lo erano.

In conclusione, in $(a \ b)^{\circ} f$ vi è un numero di inversioni superiore o inferiore di 1 rispetto a quello di f, e quindi la tesi è ovvia.

2° caso: a e b non sono adiacenti nella seconda riga di f, cioè:

$$f = \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & \dots & i_k & a & t_1 & \dots & \dots & t_s & b & j_1 & \dots & \dots & j_r \end{pmatrix}$$

La composizione sarà:

$$(a \ b)^{\circ} f = \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & \dots & i_k & b & t_1 & \dots & \dots & t_s & a & j_1 & \dots & \dots & j_r \end{pmatrix}$$

Il *passaggio* da f a $(a \ b)^{\circ} f$ si può effettuare con *passaggi intermedi*, ognuno dei quali consiste nello scambio di due numeri adiacenti nella seconda riga:

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & a & t_1 & \dots & t_s & b & j_1 & \dots & j_r \end{pmatrix} \xrightarrow{\text{Si scambiano a e } t_1} \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & t_1 & a & \dots & t_s & b & j_1 & \dots & j_r \end{pmatrix} \rightarrow \\ &\xrightarrow{\text{Si scambiano a e } t_2} \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & t_1 & t_2 & a & \dots & t_s & b & j_1 & \dots & j_r \end{pmatrix} \xrightarrow{\text{Si scambiano a e } t_3 \text{ etc. fino a quando} \\ &\quad \text{a e b sono adiacenti.}} \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & t_1 & t_2 & \dots & t_s & b & a & j_1 & \dots & j_r \end{pmatrix} \rightarrow \\ &\xrightarrow{\text{Si scambiano b e } t_s} \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & t_1 & t_2 & \dots & b & t_s & a & j_1 & \dots & j_r \end{pmatrix} \xrightarrow{\text{si scambiano quindi b e } t_{s-1} \text{ etc fino a b con } t_1} \\ &\xrightarrow{\text{Cioè fino ad ottenere:}} \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_1 & \dots & i_k & b & t_1 & \dots & \dots & t_s & a & j_1 & \dots & j_r \end{pmatrix} = (a \ b)^{\circ} f. \end{aligned}$$

Ad ogni *passaggio* la parità cambia, alternandosi tra pari e dispari. Il numero di passaggi fatti è in numero di:

s (per scambiare a con $t_1 \dots t_s$) $+1$ (per scambiare a e b) $+ s$ (per scambiare b con $t_1 \dots t_s$),
cioè, in totale, $2s+1$, che è dispari. Allora, anche in questo secondo caso la parità di $(a \ b)^{\circ} f$ è diversa da quella di f (perché aggiungendo un numero dispari di inversioni si cambia la parità) ed il lemma è dimostrato.

Lezione n°. 38 – 12 feb. 2001

Un esempio di applicazione del lemma dimostrato è il **gioco del quindici**: è un gioco la cui struttura è costituita da una *scacchiera* di 16 caselle (4 righe per 4 colonne) e con 15 *pedine* numerate da 1 a 15, inserite nelle caselle, delle quali una rimane vuota. Le *mosse* consentite sono lo spostamento in orizzontale o in verticale di una pedina nella casella vuota. Lo scopo del gioco è, attraverso le mosse consentite, di arrivare ad una configurazione della scacchiera diversa da quella iniziale *ordinata* (pedine in ordine da 1 a 15 e con la casella in basso a destra vuota) e, da questa, tornare alla configurazione iniziale.

Configurazione di partenza
e di arrivo.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Si può interpretare il gioco nel linguaggio delle permutazioni: si identifica ogni configurazione della scacchiera con una permutazione $f \in S_{16}$ nel modo seguente: si numerano le caselle da 1 a 16, partendo da sinistra in alto ed arrivando in basso a destra. Si considera quindi, oltre alle 15 pedine numerate, una pedina *jolly*, corrispondente alla casella vuota, e la si contrassegna con il numero 16. Una configurazione della scacchiera è identificata alla permutazione $f \in S_{16}$ che associa ad ogni casella la pedina che la occupa.

$$f = \left(\begin{array}{cccccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{array} \right) \begin{array}{l} \leftarrow \text{caselle} \\ \leftarrow \text{pedine} \end{array}$$

La configurazione iniziale (cioè quella *ordinata*) corrisponde alla permutazione identica. Interpretiamo una mossa nel linguaggio delle permutazioni: se $f \in S_{16}$ è una configurazione, con una mossa si ottiene una nuova configurazione $f' \in S_{16}$. La f' è legata alla f dal fatto

che la pedina n°. 16 viene scambiata con un'altra pedina n° x (in pratica una mossa equivale all'applicazione di una trasposizione), quindi $f'=(16\ x)^o f$.

Questo comporta delle limitazioni nelle configurazioni che si possono ottenere a partire da quella iniziale. Per esempio, una configurazione (ottenuta a partire da quella iniziale) in cui la casella 16 è vuota (cioè è rimasta *ferma*) è sempre una permutazione pari. Infatti il numero di mosse necessario per arrivare ad una tale configurazione è sempre pari. Ciò si dimostra osservando che la pedina n°. 16, ad ogni mossa, può muoversi o verso l'alto, o verso il basso, o verso destra o verso sinistra ma, per ritrovarsi alla fine nella casella n°. 16, il numero di mosse verso l'alto deve essere uguale al numero di mosse verso il basso, e lo stesso discorso vale per le mosse a destra e sinistra, per cui il numero di mosse finale è pari. Se k è tale numero di mosse (con k pari), la situazione delle mosse è la seguente: all'inizio si ha la permutazione identica che, composta con una trasposizione (1^a mossa) da luogo ad una nuova configurazione (permutazione) che, composta con un'altra trasposizione (2^a mossa) da luogo ad un'ulteriore configurazione, generata quindi dalla composizione di due trasposizioni con la permutazione identica, e così via. Ora, il lemma prima dimostrato dice che ad ogni composizione con una trasposizione (cioè ad ogni mossa) la parità della permutazione cambia (da pari a dispari e viceversa) e quindi alla fine, essendo pari il numero k di mosse, la permutazione finale avrà la stessa parità di quella iniziale, che è la permutazione identica (che è pari). Quindi la permutazione (configurazione) finale è anch'essa pari, così come tutte quelle che si possono ottenere a partire da quella ordinata (e che abbiano la casella n°. 16 vuota).

Esempio:

la seguente configurazione non si può ottenere a partire da quella inizialmente ordinata, perché presenta una sola inversione in 14,15 e quindi è una permutazione dispari.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Equivale a $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 15 & 14 & 16 \end{smallmatrix} \right)$

Conseguenze matematiche del lemma.

1. data una permutazione $f \in S_n$ e, scomposta f in trasposizioni, cioè:

$$f = (a \ b)^{\circ} (c \ d)^{\circ} (e \ f)^{\circ} \dots \dots^{\circ} (r \ s)$$

allora f è pari se il numero di trasposizioni è pari, mentre è dispari se il numero di trasposizioni è dispari. Infatti, se i è la permutazione identica, basta ricordare che $f^{\circ}i = f$ e che quindi $f = f^{\circ}i = (a \ b)^{\circ} (c \ d)^{\circ} (e \ f)^{\circ} \dots \dots^{\circ} (r \ s)^{\circ} i$ e, ricordando che ad ogni composizione con una trasposizione la parità cambia (lemma), essendo i una permutazione pari, si ottiene la tesi.

Esempio:

$$f = \left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 7 & 6 & 4 & 9 & 8 \end{array} \right) \in S_9$$

Per controllare la parità della f basta scomporla in trasposizioni e contarle:

$$f = (1 \ 3 \ 2)^{\circ} (4 \ 5 \ 7)^{\circ} (8 \ 9) = (1 \ 2)^{\circ} (1 \ 3)^{\circ} (4 \ 7)^{\circ} (4 \ 5)^{\circ} (8 \ 9)$$

La f è scomposta in 5 trasposizioni per cui è una permutazione dispari.

2. La parità di un ciclo dipende dalla sua lunghezza, nel senso che:

- se la lunghezza è pari il ciclo è dispari;
- se la lunghezza è dispari il ciclo è pari;

Infatti se f è il ciclo di lunghezza k si ha: $f = (i_1 \ i_2 \ i_3 \ \dots \ i_k)$ che può essere scomposto in $(k-1)$ trasposizioni (i_1 si *accoppia* con tutti gli altri $k-1$ numeri ma non con se stesso):

$$f = (i_1 \ i_k)^{\circ} (i_1 \ i_{k-1})^{\circ} \dots \dots^{\circ} (i_1 \ i_3)^{\circ} (i_1 \ i_2).$$

Quindi il ciclo di lunghezza k è scomposto in $(k-1)$ trasposizioni, per cui la parità del ciclo dipende da $(k-1)$ (basta guardare al punto 1) e quindi la tesi.

Lezione n°. 39 – 14 feb. 2001

Regola per la parità della composizione di permutazioni.

Se $f, g \in S_n$, con f e g pari o dispari, che cosa si può dire sulla parità della composizione $f^{\circ}g$?

La risposta è data dal seguente teorema:

teorema: se f e g sono entrambe pari o entrambe dispari, allora $f^{\circ}g$ è ancora pari o dispari; se f e g sono una pari e l'altra dispari allora $f^{\circ}g$ è dispari. (la regola è uguale alla regola della somma di numeri pari e dispari).

Dimostrazione: per una conseguenza del lemma precedente, la parità di una permutazione dipende dalla parità del numero di trasposizioni in cui essa si può decomporre. Quindi, se f si decompone in k trasposizioni ($f = (a_1 \ b_1)^{\circ} (a_2 \ b_2)^{\circ} \dots (a_k \ b_k)^{\circ}$) e g si decompone in h trasposizioni ($g = (c_1 \ d_1)^{\circ} (c_2 \ d_2)^{\circ} \dots (c_h \ d_h)^{\circ}$), allora $f^{\circ}g$ si decompone in $(k+h)$

trasposizioni: $f^o g = (a_1 b_1)^o (a_2 b_2)^o \dots (a_k b_k)^o (c_1 d_1)^o (c_2 d_2)^o \dots (c_h d_h)^o$ e quindi si ha la tesi (se k ed h sono entrambi numeri pari o entrambi dispari segue che $k+h$ è pari, mentre se sono di parità diversa la somma è dispari).

Determinante di una matrice quadrata.

Data una matrice con n righe ed m colonne (brevemente $m \times n$), si dice che essa è una **matrice quadrata** se $n=m$ (cioè se ha lo stesso numero di righe e di colonne). Sia data una matrice quadrata $n \times n$, in cui le caselle sono riempite con numeri arbitrari; si assocerà a tale matrice un numero, detto **determinante** della matrice quadrata. Indichiamo con il simbolo a_{ij} il generico elemento della matrice nella casella all'incrocio tra la riga i e la colonna j . Con tale convenzione, una matrice quadrata 2×2 sarà:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

una matrice 3×3 sarà così:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

e così via.

Consideriamo nella matrice $n \times n$ un prodotto di n elementi tutti scelti in righe e colonne diverse (cioè nessuno di questi elementi deve stare nella stessa riga o nella stessa colonna di un altro). Per esempio, nella matrice 3×3 , si può considerare il prodotto:

$a_{11} * a_{23} * a_{32}$. Quanti sono tutti i possibili prodotti siffatti? Uno di tali prodotti si può costruire formalmente prendendo un elemento nella 1ª riga, uno nella 2ª e così via, quindi è un prodotto del tipo: $a_{1?} * a_{2?} * a_{3?} * \dots * a_{n?}$, dove i simboli '?' indicano le colonne in cui si sceglieranno gli elementi. Poiché le colonne devono anch'esse essere diverse tra loro, i '?' saranno i numeri interi da 1 ad n in un certo ordine. Quindi il prodotto costruito con tale criterio avrà la forma:

$a_{1i_1} * a_{2i_2} * a_{3i_3} * \dots * a_{ni_n}$ dove $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$, che è una permutazione in S_n .

Quindi, in totale, in corrispondenza delle permutazioni in S_n , si ottengono $n!$ possibili prodotti costruiti con il criterio precedente.

Esempio: in una matrice 2×2 si ottengono $2!=2$ prodotti:

$$\begin{array}{ccc} a_{11} * a_{22} & \text{e} & a_{12} * a_{21} \\ \downarrow & & \downarrow \\ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} & & \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \end{array}$$

In una matrice 3x3 si ottengono $3!=6$ prodotti:

$$\begin{array}{cccccc}
 a_{11} * a_{22} * a_{33} & a_{13} * a_{21} * a_{32} & a_{12} * a_{23} * a_{31} & a_{11} * a_{23} * a_{32} & a_{13} * a_{22} * a_{31} & a_{12} * a_{21} * a_{33} \\
 \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}
 \end{array}$$

Etc.

Per definizione, il **determinante di una matrice quadrata $n \times n$** è quel numero ottenuto sommando tutti i prodotti di n elementi in righe e colonne diverse, ognuno preso con il suo segno, se la permutazione corrispondente è pari, con il segno opposto, se la permutazione corrispondente è dispari.

Esempi:

in una matrice 2x2 il determinante è $a_{11} * a_{22} - a_{12} * a_{21}$ (la permutazione corrispondente al primo prodotto è la permutazione identica che è pari, la permutazione corrispondente al secondo prodotto è dispari perché presenta la sola inversione 2,1).

In pratica, solo per le matrici 2x2, il determinante è la differenza dei prodotti “in croce”, cioè dei prodotti degli elementi che si trovano lungo le diagonali)

In una matrice 3x3 il determinante è:

$$\begin{array}{cccccc}
 a_{11} * a_{22} * a_{33} & + & a_{13} * a_{21} * a_{32} & + & a_{12} * a_{23} * a_{31} & - & a_{11} * a_{23} * a_{32} & - & a_{13} * a_{22} * a_{31} & - & a_{12} * a_{21} * a_{33} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\
 \text{Pari} & & \text{pari} & & \text{pari} & & \text{dispari} & & \text{dispari} & & \text{dispari}
 \end{array}$$

Anche per le matrici 3x3 il determinante c'è una regola pratica per il calcolo del determinante: si ricopiano le prime due righe sotto le altre e si prendono i 6 prodotti nelle diagonali, con il loro segno quelli lungo le diagonali da sinistra a destra e con il segno opposto quelli lungo le diagonali da destra a sinistra.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

Per le matrici 4x4 o più, si usa un metodo di calcolo detto **Sviluppo di Laplace**.

Sviluppo di Laplace.

Si basa sul concetto di **minore estratto da una matrice**; sia data una matrice $n \times m$ (quindi non necessariamente quadrata): se si fissa all'interno della matrice un certo numero k di righe e colonne e se si considerano gli elementi appartenenti a tali k righe e k colonne dalla matrice, tali elementi *estratti* dalla matrice formano a loro volta una matrice quadrata $k \times k$, il cui determinante è detto **minore di ordine k estratto dalla matrice di partenza**.

Esempio: nella matrice 3x4 seguente:

$$\begin{pmatrix} 1 & 2 & 5 & 7 \\ -2 & 3 & 4 & 1 \\ 0 & 2 & 5 & -3 \end{pmatrix}$$
 Se fissiamo 2 righe e 2 colonne ($k=2$), ad esempio la prima e la terza riga e la terza e quarta colonna, possiamo prendere gli elementi comuni a queste righe e colonne che formano la seguente matrice 2x2:

$$\begin{pmatrix} 5 & 7 \\ 5 & -3 \end{pmatrix}$$

il cui determinante è $-15-35=-50$, che è il minore di ordine 2 estratto dalla matrice data.

Definiamo adesso il concetto di **complemento algebrico di un elemento di una matrice quadrata**. Se è data una matrice quadrata $n \times n$, fissato un elemento a_{ij} , consideriamo le rimanenti $n-1$ righe ed $n-1$ colonne in cui l'elemento a_{ij} non compare; tali righe e colonne determinano un minore di ordine $n-1$. si definisce complemento algebrico dell'elemento a_{ij} tale minore, preso con il suo segno se la somma $i+j$ è pari, con il segno opposto se la somma $i+j$ è dispari.

Esempio: sia data la matrice 3x3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & -2 & 1 \\ 3 & -5 & 3 \end{pmatrix}$$

Preso ad esempio $a_{23}=1$, si considerano gli elementi delle altre righe e colonne (escludendo la 2ª riga e la 3ª colonna), che formano la matrice seguente 2x2:

$$\begin{pmatrix} 1 & 2 \\ 3 & -5 \end{pmatrix}$$

Il determinante di tale matrice è $-5-6=-11$, ed è il minore di ordine 2 della matrice data. Poiché la somma degli indici dell'elemento scelto $a_{23}=1$ è $2+3=5$ dispari, il complemento algebrico di a_{23} è $-(-11)=11$.

Lezione n°. 40 – 16 feb. 2001

Sviluppo di Laplace di un determinante (senza dimostrazione).

Data una matrice quadrata $n \times n$ il suo determinante si può ottenere fissando a piacere una riga o una colonna e sommando tutti i prodotti degli elementi della riga (o della colonna) moltiplicati per i loro complementi algebrici (*operativamente* conviene fissare una riga o colonna nella quale siano presenti alcuni elementi nulli).

Esempio:

calcoliamo il determinante della matrice 5x5:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 5 \\ 2 & 0 & 2 & 0 & 1 \\ 5 & -1 & 1 & 2 & -2 \\ 1 & 2 & 3 & 1 & 3 \\ 3 & 0 & 1 & 2 & 1 \end{pmatrix}$$

Fissata la seconda colonna (che contiene 3 zeri) basta sommare i prodotti degli elementi non nulli (-1 e 2) per i loro complementi algebrici:

Il complemento algebrico di -1 è il determinante della matrice:

$$\begin{pmatrix} 1 & 0 & 3 & 5 \\ 2 & 2 & 0 & 1 \\ 1 & 3 & 1 & 3 \\ 3 & 1 & 2 & 1 \end{pmatrix}$$

che va preso con il segno opposto perché -1 è l'elemento a_{32} e $3+2$ è dispari.

Il complemento algebrico di 2 è il determinante della matrice:

$$\begin{pmatrix} 1 & 0 & 3 & 5 \\ 2 & 2 & 0 & 1 \\ 5 & 1 & 2 & -2 \\ 3 & 1 & 2 & 1 \end{pmatrix}$$

che va preso con il proprio opposto perché 2 è l'elemento a_{42} e $4+2$ è pari.

Quindi si calcolano i determinanti delle matrici 4×4 etc.

Sistemi lineari di equazioni.

Di questo argomento si affronta solo qualche aspetto.

Un sistema lineare quadrato è un sistema di n equazioni in n incognite, in cui tutti i monomi (tranne il termine noto) sono di 1° grado. Formalmente un tale sistema si rappresenta come segue:

[illegible]

dove x_1, x_2, \dots, x_n sono le incognite, a_{ij} indica il coefficiente dell'incognita x_j nell'equazione i e $b_1 \dots b_n$ sono i termini noti.

Risolvere un tale sistema (se è possibile) significa trovare dei valori numerici da attribuire alle incognite che soddisfino contemporaneamente tutte le equazioni.

Dato il sistema precedente si chiama **matrice del sistema** la matrice quadrata $n \times n$ ottenuta considerando solo i coefficienti delle incognite:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Il determinante di questa matrice si indica con Δ .

Sostituendo ad una ad una le colonne della matrice del sistema con la colonna dei termini noti, si ottengono altre n matrici $n \times n$, dette **matrici ausiliarie**.

$$\begin{pmatrix} b_1 & a_{12} & \dots & a_{1n} \\ b_2 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ b_n & a_{n2} & \dots & a_{nn} \end{pmatrix} \text{ il cui determinante si indica con } \Delta_1,$$

$$\begin{pmatrix} a_{11} & b_1 & \dots & a_{1n} \\ a_{21} & b_2 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & b_n & \dots & a_{nn} \end{pmatrix} \text{ il cui determinante si indica con } \Delta_2,$$

.....

$$\begin{pmatrix} a_{11} & a_{12} & \dots & b_1 \\ a_{21} & a_{22} & \dots & b_2 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & b_n \end{pmatrix} \text{ il cui determinante si indica con } \Delta_n.$$

Teorema di Cramer (senza dimostrazione).

Se il determinante Δ della matrice dei coefficienti è non nullo, allora il sistema ha un'unica soluzione ottenuta da: $x_1 = \Delta_1 / \Delta$, $x_2 = \Delta_2 / \Delta$, ... $x_n = \Delta_n / \Delta$.

Esempio: risolvere (se possibile) il seguente sistema quadrato di 4 equazioni in 4 incognite:

$$\begin{cases} x_1 - x_2 + x_3 = 1 \\ x_2 + 3x_4 = 2 \\ x_3 - x_4 = 5 \\ x_1 + 2x_2 + 3x_3 - x_4 = 0 \end{cases}$$

Verifichiamo se si può applicare il teorema di Cramer, vediamo cioè se il determinante della matrice dei coefficienti è non nullo:

$$\begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \\ 1 & 2 & 3 & -1 \end{pmatrix}$$

Per calcolare il determinante Δ si sviluppa con il metodo di Laplace, fissando, ad esempio, la prima colonna:

il complemento algebrico dell'elemento $a_{11}=1$ è il determinante (preso con il suo segno) della matrice:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -1 \\ 2 & 3 & -1 \end{pmatrix}$$

il complemento algebrico dell'elemento $a_{41}=1$ è il determinante (preso con il segno opposto) della matrice:

$$\begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 3 \\ 0 & 1 & -1 \end{pmatrix}$$

Calcoliamo i determinanti delle due matrici 3×3 (con il metodo della ricopiatura delle prime due righe):

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -1 \\ 2 & 3 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 1 \end{pmatrix} \text{ il determinante è uguale a } -1-6+3=-4$$

$$\begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 3 \\ 0 & 1 & -1 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix} \text{ il determinante è } -4, \text{ infatti } 3+1=4 \text{ (ma è da prendere con il segno opposto).}$$

Quindi il determinante $\Delta=1*(-4)+1*(-4)= -8$, è diverso da zero per cui il teorema di Cramer può essere applicato; il sistema ammette una sola soluzione data da:

$$x_1=\Delta_1/\Delta, \quad x_2=\Delta_2/\Delta, \quad x_3=\Delta_3/\Delta, \quad x_4=\Delta_4/\Delta.$$

$$\Delta_1=\text{determinante di } \begin{pmatrix} 1 & -1 & 1 & 0 \\ 2 & 1 & 0 & 3 \\ 5 & 0 & 1 & -1 \\ 0 & 2 & 3 & -1 \end{pmatrix} = \dots=84 \Rightarrow x_1=\Delta_1/\Delta= -84/8$$

$$\Delta_2=\text{determinante di } \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 5 & 1 & -1 \\ 1 & 0 & 3 & -1 \end{pmatrix} = \dots=35 \Rightarrow x_2=\Delta_2/\Delta= -35/8$$

$$\Delta_3=\text{determinante di } \begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 5 & -1 \\ 1 & 2 & 0 & -1 \end{pmatrix} = \dots= -57 \Rightarrow x_3=\Delta_3/\Delta= 57/8$$

$$\Delta_4 = \text{determinante di } \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 5 \\ 1 & 2 & 3 & 0 \end{pmatrix} = \dots = -17 \Rightarrow x_4 = \Delta_4 / \Delta = 17/5$$

Sostituendo queste soluzioni nel sistema si verifica se sono esatte, cioè se tutte le equazioni sono valide contemporaneamente.

$$-84/8 + 35/8 + 57/8 = 8/8 = 1$$

$$-35/8 + 3 \cdot (17/8) = (-35 + 51)/8 = 16/8 = 2$$

$$57/8 - 17/8 = 40/8 = 5$$

$$-84/8 + 2 \cdot (-35/8) + 3 \cdot (57/8) = (-84 - 70 + 151)/8 = 0/8 = 0$$

Lezione n°. 41 – 19 feb. 2001

Si è visto che, secondo il teorema di Cramer, un sistema di n equazioni in n incognite ammette un'unica soluzione se il determinante Δ della matrice dei coefficienti è non nullo, e che le soluzioni sono date da $x_1 = \Delta_1 / \Delta$, $x_2 = \Delta_2 / \Delta$ $x_n = \Delta_n / \Delta$, dove i Δ_i sono i determinanti delle matrici ottenute dalla matrice dei coefficienti sostituendo alla colonna i la colonna dei termini noti.

Vediamo adesso cosa succede quando il determinante Δ è nullo. Per risolvere questo quesito bisogna introdurre il concetto di *rango di una matrice*.

Rango di una matrice.

Sia data una matrice $m \times n$ (non necessariamente quadrata). Sappiamo che, fissato un intero k (non maggiore né di n né di m), si può costruire una matrice quadrata $k \times k$, ottenuta fissando a piacere k righe e k colonne della matrice di partenza, e prendendo gli elementi comuni a tali righe e colonne e che il determinante di tale matrice è detto *minore di ordine k estratto dalla matrice data*. Si definisce **rango della matrice $m \times n$** iniziale, il più grande numero k tale che si possa estrarre dalla matrice un minore di ordine k che sia diverso da zero.

Esempio:

consideriamo la matrice 3×4 :

$$\begin{pmatrix} 1 & 3 & -2 & 5 \\ 4 & 10 & -3 & 7 \\ 3 & 7 & -1 & 2 \end{pmatrix}$$

per calcolare il rango di tale radice, possiamo estrarre minori di ordine 3, ma si deve controllare che almeno uno di essi sia non nullo: fissiamo ad esempio le tre righe e le colonne 1, 3 e 4, ottenendo la matrice $\begin{pmatrix} 1 & -2 & 5 \\ 4 & -3 & 7 \\ 3 & -1 & 2 \end{pmatrix}$ il cui determinante è:

$$\det \begin{pmatrix} 1 & -2 & 5 \\ 4 & -3 & 7 \\ 3 & -1 & 2 \end{pmatrix} = -6 - 20 - 42 + 45 + 7 + 16 = 0$$

Si verifica che tutti i minori di ordine 3 che si possono estrarre dalla matrice sono nulli (in tutto sono 4):

$$\det \begin{pmatrix} 1 & 3 & -2 \\ 4 & 10 & -3 \\ 3 & 7 & -1 \end{pmatrix} = -10 - 56 - 27 + 60 + 21 + 12 = 0 \text{ (le 3 righe e le colonne 1, 2 e 3);}$$

$$\det \begin{pmatrix} 1 & 3 & 5 \\ 4 & 10 & 7 \\ 3 & 7 & 2 \end{pmatrix} = 20 + 140 + 63 - 150 - 49 - 24 = 0 \text{ (le 3 righe e le colonne 1, 2 e 4);}$$

$$\det \begin{pmatrix} 3 & -2 & 5 \\ 10 & -3 & 7 \\ 7 & -1 & 2 \end{pmatrix} = -18 - 50 - 98 + 105 + 21 + 40 = 0 \text{ (le 3 righe e le colonne 2, 3 e 4)}$$

Si può quindi concludere che il rango non è uguale a 3. Proviamo a vedere se è uguale a 2. Estraiamo un minore di ordine 2, ad esempio fissando le righe 1 e 2 e le colonne 1 e 2 ottenendo la matrice:

$$\begin{pmatrix} 1 & 3 \\ 4 & 10 \end{pmatrix} \text{ che ha determinante uguale a } 10 - 12 = -2 \text{ che è diverso da zero.}$$

Allora il rango della matrice data è uguale a 2.

Teorema di Rouchè-Capelli (senza dimostrazione).

Sia dato un sistema lineare quadrato di n equazioni in n incognite, nel quale il determinante Δ della matrice dei coefficienti sia nullo (quindi non si può applicare il teorema di Cramer). Allora, considerate le 2 matrici:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \text{ (dei coefficienti delle incognite)}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & b_n \end{pmatrix} \text{ (dei coefficienti con l'aggiunta della colonna dei termini noti)}$$

si ha che:

1. se le 2 matrici hanno rango diverso, il sistema non ha nessuna soluzione;
2. se le 2 matrici hanno rango uguale, il sistema ha infinite soluzioni.

Vediamo, nel caso in cui le due matrici abbiano rango uguale, come si trovano le infinite soluzioni. Illustriamo l'algoritmo con un esempio, considerando un sistema lineare di 3 equazioni in 3 incognite.

$$\begin{cases} x_1 + 2x_2 - x_3 = 1 \\ 2x_1 + 3x_2 - 6x_3 = -5 \\ 3x_1 + 5x_2 - 7x_3 = -4 \end{cases}$$

Calcoliamo il Δ , cioè il determinante della matrice dei coefficienti: $\begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & -6 \\ 3 & 5 & -7 \end{pmatrix}$

$$\Delta = -21 - 10 - 36 + 9 + 30 + 28 = 0.$$

Allora, per il teorema di Rouchè-Capelli si devono calcolare i ranghi delle due matrici:

$$\text{Rango} \begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & -6 \\ 3 & 5 & -7 \end{pmatrix} = 2 \text{ perché c'è un solo minore di ordine 3 (il determinante della matrice}$$

stessa, che abbiamo visto essere nullo) mentre ci sono minori di ordine 2 non nulli (ad esempio fissando le righe 1 e 2 e le colonne 1 e 2, il determinante è $3 - 4 = -1$).

$$\text{Rango} \begin{pmatrix} 1 & 2 & -1 & 1 \\ 2 & 3 & -6 & -5 \\ 3 & 5 & -7 & -4 \end{pmatrix} = 2 \text{ perché ci sono 4 minori di ordine 3 ma sono tutti nulli (si può}$$

verificare facilmente), mentre ci sono minori di ordine 2 non nulli (ad esempio fissando le righe 1 e 2 e le colonne 1 e 2, il determinante è $3 - 4 = -1$).

Allora i ranghi delle due matrici sono uguali e quindi il sistema ammette infinite soluzioni.

Per calcolare tali soluzioni si applica il seguente metodo:

1. si individuano le k righe e le k colonne che hanno permesso di trovare un minore di ordine k non nullo (se il rango è k). Nel nostro esempio sono le righe 1 e 2 e le colonne 1 e 2;
2. si isolano le k incognite corrispondenti alle k colonne individuate (nel nostro esempio sono quindi le incognite x_1 ed x_2). Le incognite rimanenti (nel nostro esempio x_3), si

trattano come se fossero dei termini noti e si portano al secondo membro dell'equazione.

Nel nostro esempio si ha quindi:
$$\begin{cases} x_1 + 2x_2 = 1 + x_3 \\ 2x_1 + 3x_2 = -5 + 6x_3 \end{cases}$$

si ottiene quindi un sistema quadrato di k equazioni in k incognite (nell'esempio k=2), in cui il determinante della matrice dei coefficienti è non nullo, visto che coincide con il minore fissato per determinare il rango k.

Si può quindi applicare il teorema di Cramer per risolvere tale sistema:

$$\Delta = \det \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} = -1; \Delta_1 = \det \begin{pmatrix} 1+x_3 & 2 \\ -5+6x_3 & 3 \end{pmatrix} = 3+x_3+10-12x_3 = 13-9x_3; \Delta_2 = \det \begin{pmatrix} 1 & 1+x_3 \\ 2 & -5+6x_3 \end{pmatrix} = -5+6x_3-2-2x_3 = -7+4x_3$$

Quindi:

$$x_1 = \Delta_1 / \Delta = (13-9x_3) / (-1) = 9x_3 - 13$$

$$x_2 = \Delta_2 / \Delta = (-7+4x_3) / (-1) = 7-4x_3$$

Si ottengono infinite soluzioni per il sistema iniziale perché all'incognita x_3 si può attribuire un valore arbitrario, in funzione del quale si trovano i valori di x_1 ed x_2 .

Lezione n°. 42 – 21 feb. 2001

Principio di inclusione-esclusione.

Siano A e B due insiemi finiti rispettivamente di ordine n ed m; calcoliamo l'ordine dell'unione dei due insiemi. Se A e B non hanno elementi in comune (cioè $A \cap B = \emptyset$) allora è ovvio che $|A \cup B| = |A| + |B|$ (**principio della somma**).

Se invece $A \cap B \neq \emptyset$, non dovendosi contare due volte gli elementi comuni, si ha:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Esempio: se $A = \{a, b, c, d, e\}$ e $B = \{a, c, f, g\}$ si ha $A \cup B = \{a, b, c, d, e, f, g\}$ (gli elementi comuni a e c si contano una sola volta e quindi, in questo caso $|A \cup B| = |A| + |B| - |A \cap B| = 5 + 5 - 2 = 7$

La formula $|A \cup B| = |A| + |B| - |A \cap B|$ è detta **principio di inclusione-esclusione** (si *includono* gli elementi di A e B e si *escludono* quelli comuni). Notare che il principio della somma altro non è che il caso particolare del principio di inclusione-esclusione in cui $|A \cap B| = 0$ (in quanto l'ordine di \emptyset è zero).

Il principio di inclusione-esclusione si generalizza per l'unione di più di 2 insiemi finiti: siano dati, ad esempio, 3 insiemi finiti A, B e C e calcoliamo $|A \cup B \cup C|$; notando che $A \cup B \cup C = (A \cup B) \cup C$ (proprietà associativa dell'unione di insiemi) si può applicare il principio valido per 2 insiemi, ottenendo: $|A \cup B \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$, considerando cioè

(AUB) come il primo insieme e C come il secondo. Sappiamo già che $|AUB|=|A|+|B|-|A\cap B|$ ed inoltre che, per la proprietà distributiva si ha che $(AUB)\cap C=(A\cap C)\cup(B\cap C)$, quindi:

$$|(A\cap C)\cup(B\cap C)|=|A\cap C|+|B\cap C|-|A\cap B\cap C|.$$

Componendo i termini trovati si ottiene la formula valida per calcolare l'ordine dell'unione di 3 insiemi finiti: $|A\cup B\cup C|=|A|+|B|+|C|-(|A\cap B|+|A\cap C|+|B\cap C|)+|A\cap B\cap C|$.

Iterando il procedimento si ottiene una formula valida per il calcolo dell'ordine dell'unione di un numero generico n di insiemi finiti $A_1, A_2, A_3, \dots, A_n$:

$|A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \dots \pm \alpha_n$, dove i simboli $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ hanno i seguenti significati:

- α_1 =somma degli ordini dei singoli insiemi, cioè $|A_1|+|A_2|+|A_3|+\dots+|A_n|$;
- α_2 =somma degli ordini delle intersezioni a 2 a 2, cioè: $|A_1\cap A_2|+|A_1\cap A_3|+\dots+|A_{n-1}\cap A_n|$;
- α_3 =somma degli ordini delle possibili intersezioni a 3 a 3, cioè:

$$|A_1\cap A_2\cap A_3|+|A_1\cap A_2\cap A_4|+\dots+|A_{n-2}\cap A_{n-1}\cap A_n|;$$

.....

- α_n =somma (con un solo termine) degli ordini delle intersezioni ad n ad n, cioè:

$$|A_1\cap A_2\cap A_3\cap \dots \cap A_n|;$$

e dove il segno \pm dell'ultimo addendo α_n dipende da n (se n è dispari sarà un numero positivo, se è pari sarà un numero negativo).

Il principio di inclusione-esclusione ha una applicazione "positiva" ed una applicazione "negativa":

1. applicazione "positiva": dato un insieme finito A, si debbano contare quanti elementi di A **soddisfano** almeno una fra n proprietà date. Se si pone:

$$A_1=\{x\in A / x \text{ soddisfa la proprietà 1}\},$$

$$A_2=\{x\in A / x \text{ soddisfa la proprietà 2}\},$$

.....

$$A_n=\{x\in A / x \text{ soddisfa la proprietà n}\},$$

il problema dato equivale al calcolo di $|A_1 \cup A_2 \cup \dots \cup A_n|$, quindi con l'applicazione del principio di inclusione-esclusione.

Esempio: sia A l'insieme delle parole (disposizioni con ripetizione) di lunghezza 6 sull'alfabeto $\{a,b,c,d\}$; quante sono le parole di A che soddisfano almeno una delle seguenti proprietà?

- 1) La prima lettera è d;
- 2) L'ultima lettera è a;
- 3) La quarta lettera è c.

Soluzione:

basta porre:

$$A_1 = \{x \in A / x \text{ soddisfa la proprietà 1}\},$$

$$A_2 = \{x \in A / x \text{ soddisfa la proprietà 2}\},$$

$$A_3 = \{x \in A / x \text{ soddisfa la proprietà 3}\},$$

e calcolare $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|$.

Calcoliamo i singoli addendi:

$|A_1|$ = numero di parole di A che hanno la prima lettera uguale a d, che sono in numero di 4^5 (disposizioni con ripetizione di 4 lettere prese a 5 a 5). Analogamente $|A_2| = |A_3| = 4^5$.

$|A_1 \cap A_2|$ = numero di parole di A che hanno la prima lettera uguale a d e l'ultima lettera uguale ad a, cioè le disposizioni con ripetizione di 4 lettere prese a 4 a 4 che sono in numero di 4^4 . Per lo stesso ragionamento $|A_1 \cap A_3| = |A_2 \cap A_3| = 4^4$.

$|A_1 \cap A_2 \cap A_3|$ = numero di parole di A che hanno la prima lettera uguale a d, la quarta uguale a c e l'ultima uguale ad a, cioè le disposizioni con ripetizione di 4 lettere prese a 3 a 3 che sono in numero di 4^3 . Quindi in totale si ha che $|A_1 \cup A_2 \cup A_3| = 3 \cdot 4^5 - 3 \cdot 4^4 + 4^3$.

2. applicazione "negativa": se A è un insieme finito, si voglia calcolare il numero di elementi di A che **non soddisfano** nessuna di n proprietà date.

Anche in questo caso, se si pone:

$$A_1 = \{x \in A / x \text{ soddisfa la proprietà 1}\},$$

$$A_2 = \{x \in A / x \text{ soddisfa la proprietà 2}\},$$

.....

$$A_n = \{x \in A / x \text{ soddisfa la proprietà n}\},$$

si dovranno contare gli elementi che sono esterni a tutti gli insiemi A_1, A_2, \dots, A_n , cioè il complementare dell'unione di questi insiemi. Quindi il problema equivale al calcolo dell'ordine del complementare di $(A_1 \cup A_2 \cup \dots \cup A_n)$, cioè il calcolo di $|A| - |A_1 \cup A_2 \cup \dots \cup A_n|$, dove si usa il principio di inclusione-esclusione.

Lezione n°. 43 – 23 feb. 2001

Esempio: il "Problema della segretaria distratta". Date n buste nelle quali si devono inserire n lettere (tutte con destinatari diversi), in quanti modi diversi si può sbagliare del tutto l'inserimento delle lettere nelle buste (cioè nessuna lettera nella busta giusta)?

Numeriamo tutte le lettere e tutte le buste da 1 ad n (lettere e buste corrispondenti avranno lo stesso numero).

Ogni modo di inserire le lettere nelle buste corrisponde ad una applicazione biunivoca di S_n :

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \begin{matrix} \leftarrow \text{lettere} \\ \leftarrow \text{buste} \end{matrix}$$

Quindi il numero di modi possibili di inserire le lettere nelle buste sono in numero di $n!$ (cioè il numero di possibili applicazioni biunivoche). Il problema richiede di contare le permutazioni $f \in S_n$ che non soddisfano nessuna delle seguenti proprietà:

$$f(1)=1, f(2)=2, \dots, f(n)=n.$$

Si usa l'applicazione *negativa* del principio di inclusione-esclusione, e si pone:

$$A_1 = \{x \in A \mid x \text{ soddisfa la proprietà 1, cioè } f(1)=1\},$$

$$A_2 = \{x \in A \mid x \text{ soddisfa la proprietà 2, cioè } f(2)=2\},$$

.....

$$A_n = \{x \in A \mid x \text{ soddisfa la proprietà } n, \text{ cioè } f(n)=n\}.$$

Il problema richiede di calcolare l'ordine del complementare dell'unione di $A_1 \cup A_2 \cup \dots \cup A_n$; la risposta al problema è quindi: $|S_n| - |A_1 \cup A_2 \cup \dots \cup A_n| = n! - |A_1 \cup A_2 \cup \dots \cup A_n|$.

Per il principio di inclusione-esclusione si ha: $|A_1 \cup A_2 \cup \dots \cup A_n| = \alpha_1 + \alpha_2 - \alpha_3 + \dots \pm \alpha_n$, (dove se n è pari si ha che α_n è di segno negativo mentre se n è dispari α_n è di segno positivo) e dove i simboli α_i hanno i seguenti significati:

- $\alpha_1 = |A_1| + |A_2| + |A_3| + \dots + |A_n|$;
- $\alpha_2 = |A_1 \cap A_2| + |A_1 \cap A_3| + \dots$;
- $\alpha_3 = |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \dots$, etc.;

calcoliamo gli α_i :

$|A_1|$ rappresenta il numero di tutte le applicazioni biunivoche da $\{2 \dots n\}$ in $\{2 \dots n\} = (n-1)!$, infatti si tratta di tutte le possibili permutazioni di S_n in cui è fissato solo $f(1)=1$.

Lo stesso ragionamento vale per $|A_2| = |A_3| = |A_4| = \dots = |A_n| = (n-1)!$, in quanto ogni addendo rappresenta il numero di tutte le permutazioni di S_n con, di volta in volta, è fissato $f(i)=i$.

In conclusione, quindi, il termine $\alpha_1 = |A_1| + |A_2| + |A_3| + \dots + |A_n| = n \cdot (n-1)! = n!$, essendo la somma di n termini uguali ad $(n-1)!$.

Per quanto riguarda il termine α_2 osserviamo che $|A_1 \cap A_2|$ rappresenta il numero di tutte le applicazioni biunivoche da $\{3 \dots n\}$ in $\{3 \dots n\} = (n-2)!$, infatti si tratta di tutte le possibili permutazioni di S_n in cui sono fissati solo $f(1)=1$ ed $f(2)=2$. Lo stesso ragionamento vale per ogni altro addendo di α_2 in quanto ognuno rappresenta il numero di permutazioni possibili di S_n in cui, di volta in volta, sono fissati due elementi $f(i)=i$ ed $f(j)=j$. Il numero di

addendi di α_2 è il numero di intersezioni a 2 a 2 possibili tra n insiemi, cioè le combinazioni semplici di n elementi presi a 2 a 2, che è pari a:

$$\text{In conclusione, quindi: } \alpha_2 = \binom{n}{2} * (n-2)!$$

Con un ragionamento analogo si giunge alla determinazione dei valori degli altri termini α_i :

$$\alpha_3 = \binom{n}{3} * (n-3)! \quad \alpha_4 = \binom{n}{4} * (n-4)! \quad \text{etc.}$$

$$\text{In generale si avrà: } \alpha_i = \binom{n}{i} * (n-i)! = \frac{n!}{i!(n-i)!} * (n-i)! = \frac{n!}{i!}$$

$$\text{Quindi: } \alpha_2 = n!/2!, \alpha_3 = n!/3!, \alpha_4 = n!/4!, \dots, \alpha_n = n!/n! = 1$$

Allora la risposta al problema della segretaria distratta sarà:

$$n! - |A_1 \cup A_2 \cup \dots \cup A_n| = \alpha_1 + \alpha_2 - \alpha_3 + \dots \pm \alpha_n = n! - (n! - n!/2 + n!/3! - n!/4! + \dots \pm 1) = n!/2 - n!/3! + n!/4! - \dots \pm 1$$

dove, in questo caso, il segno di 1 sarà positivo se n è pari, negativo se n è dispari.

Esempio: nel caso di 5 buste e 5 lettere, cioè $n=5$, ci saranno $5!=120$ modi possibili di inserire le lettere nelle buste e, tra questi 120, quelli totalmente sbagliati saranno in numero di $5!/2! - 5!/3! + 5!/4! - 1 = 120/2 - 120/6 + 120/24 - 1 = 44$ (come si vede $n=5$ è dispari e il segno di 1 è negativo).

Lezione n°. 44 – 5 mar. 2001

Funzione di Eulero.

È un'applicazione del principio di inclusione-esclusione ed è importante negli studi sulla crittografia.

Se n è un numero intero maggiore di 1, si definisce **funzione di Eulero di n** (e si indica con $\varphi(n)$) il numero di interi x tali che $1 \leq x \leq n$ che sono coprimi con n .

Esempio: se volessimo conoscere $\varphi(6)$, gli interi x compresi tra 1 e 6 coprimi con 6 sono i numeri 1 e 5, quindi $\varphi(6)=2$.

Se volessimo conoscere $\varphi(1000)$ il calcolo si complica quindi serve un algoritmo che permetta di calcolare la funzione di Eulero più facilmente.

Un tale algoritmo si ottiene con il principio di inclusione-esclusione.

Sia $n > 1$ un intero fissato; scomponiamo n in fattori primi:

$n = p_1 p_2 p_3 \dots p_k$ (con p_i numeri primi). Associando i numeri primi uguali, si può scrivere:

$n = q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_r^{k_r}$, dove i k_i sono numeri interi maggiori di 0 e i q_i sono numeri primi distinti.

Per calcolare $\varphi(n)$ possiamo allora calcolare il numero t degli interi x compresi fra 1 ed n che non sono coprimi con n e calcolare $\varphi(n)=n-t$ (perché n sono in totale gli interi compresi tra 1 ed n). Ma un numero x non è coprimo con n quando il $\text{mcd}(x,n)=d>1$; essendo d un divisore di x e di n , ponendo $n=dc$ e fattorizzando d,c in prodotto di numeri primi, per l'unicità della fattorizzazione, i primi in cui è decomposto d sono alcuni tra i q_1, q_2, \dots, q_r (quelli in cui è decomposto n); quindi d è multiplo di qualcuno dei numeri primi q_1, q_2, \dots, q_r ; ma x è multiplo di d quindi quindi anche x è multiplo dei q_1, q_2, \dots, q_r . Allora gli x cercati sono quelli multipli di qualcuno fra i primi q_1, q_2, \dots, q_r , ossia, se poniamo:

$$A_1 = \{y / y \text{ è un intero compreso tra } 1 \text{ ed } n \text{ e } y \text{ è divisibile per } q_1\}$$

$$A_2 = \{y / y \text{ è un intero compreso tra } 1 \text{ ed } n \text{ e } y \text{ è divisibile per } q_2\}$$

.....

$$A_r = \{y / y \text{ è un intero compreso tra } 1 \text{ ed } n \text{ e } y \text{ è divisibile per } q_r\}$$

gli x cercati sono gli elementi dell'unione $A_1 \cup A_2 \cup \dots \cup A_r$ e quindi $t = |A_1 \cup A_2 \cup \dots \cup A_r|$ (e qui si usa il principio di inclusione-esclusione).

A questo punto premettiamo alcuni risultati che ci serviranno nel calcolo dei singoli addendi di $|A_1 \cup A_2 \cup \dots \cup A_r| = |A_1| + |A_2| + \dots + |A_r| - (|A_1 \cap A_2| + \dots) + (|A_1 \cap A_2 \cap A_3| + \dots) + \dots \pm |A_1 \cap A_2 \cap \dots \cap A_r|$.

Premessa 1: se p, q sono numeri primi distinti e se p, q sono entrambi divisori dell'intero positivo z , allora anche il prodotto pq è divisore di z . Infatti, calcolando il $\text{mcd}(p, q) = r$ si ha che r è divisore sia di p che di q , ma p ha come divisori solo 1 e p e allo stesso modo q ha come divisori solo 1 e q (sono numeri primi) e poiché $p \neq q$ l'unica possibilità è che $\text{mcd}(p, q) = r = 1$. Ma, per una proprietà del mcd , si può scrivere $1 = p \cdot p' + q \cdot q'$, con p' e q' interi; per ipotesi p e q sono divisori di z e quindi $z = p \cdot a$ e $z = q \cdot b$ (con a e b interi). Moltiplicando per z l'eguaglianza $1 = p \cdot p' + q \cdot q'$ si ottiene:

$$z = z \cdot p \cdot p' + z \cdot q \cdot q' = (q \cdot b) \cdot p \cdot p' + (p \cdot a) \cdot q \cdot q' = pq(bp' + aq') \Rightarrow pq \text{ è divisore di } z, \text{ cioè la tesi.}$$

Facilmente si dimostra, in modo analogo, che, dati dei numeri primi distinti p, q, \dots, w , tutti divisori dello stesso intero z positivo, anche il loro prodotto $pq \cdot \dots \cdot w$ è divisore di z .


Premessa 2: consideriamo due numeri α_1 ed α_2 e calcoliamo il prodotto seguente:

$$(1 - \alpha_1)(1 - \alpha_2) = 1 - (\alpha_1 + \alpha_2) + \alpha_1 \alpha_2.$$

$$\text{Se } \alpha_1, \alpha_2, \alpha_3 \text{ sono numeri si ha: } (1 - \alpha_1)(1 - \alpha_2)(1 - \alpha_3) = 1 - (\alpha_1 + \alpha_2 + \alpha_3) + (\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3) - \alpha_1 \alpha_2 \alpha_3.$$

In generale si ottiene che, dati i numeri $\alpha_1, \alpha_2, \dots, \alpha_n$ si ha:

$$(1 - \alpha_1)(1 - \alpha_2) \dots (1 - \alpha_n) = 1 - (\alpha_1 + \alpha_2 + \dots + \alpha_n) + (\alpha_1 \alpha_2 + \dots) - (\alpha_1 \alpha_2 \alpha_3 + \dots) + \dots \pm \alpha_1 \alpha_2 \dots \alpha_n$$



somma dei prodotti a 2 a 2 somma dei prodotti a 3 a 3.....

dove l'ultimo termine ha il suo segno se n è pari, il segno opposto se n è dispari.

Tornando al problema principale, cioè il calcolo di $t=|A_1 \cup A_2 \cup \dots \cup A_r|$, dove $n=q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_r^{k_r}$ (con q_1, \dots, q_r numeri primi distinti) e dove $A_i = \{y/y \text{ è un intero tra } 1 \text{ ed } n \text{ e } y \text{ divisibile per } q_i\}$, per il principio di inclusione-esclusione si ha che

$$t=|A_1 \cup A_2 \cup \dots \cup A_r| = |A_1| + |A_2| + \dots + |A_r| - (|A_1 \cap A_2| + \dots) + (|A_1 \cap A_2 \cap A_3| + \dots) + \dots \pm |A_1 \cap A_2 \cap \dots \cap A_r| \quad (\text{dove l'ultimo termine è positivo se } r \text{ è dispari, negativo se } r \text{ è pari}).$$

Calcoliamo i singoli addendi:

$A_1 = \{y/y \text{ è un intero tra } 1 \text{ ed } n \text{ e } y \text{ divisibile per } q_1\} = \{q_1, 2q_1, 3q_1, \dots, n=nq_1/q_1\} \Rightarrow$ (sono in numero di n/q_1 e quindi $|A_1|=n/q_1$).

Analogamente si ha che $|A_2|=n/q_2$ etc.

Passiamo alle intersezioni a 2 a 2:

$A_1 \cap A_2 = \{y/y \text{ è un intero tra } 1 \text{ ed } n \text{ e } y \text{ divisibile sia per } q_1 \text{ che per } q_2\} = (\text{premessa 1}) = \{y/y \text{ è un intero fra } 1 \text{ ed } n \text{ e } y \text{ divisibile per il prodotto } q_1 q_2\} = \{q_1 q_2, 2q_1 q_2, 3q_1 q_2, \dots, n=nq_1 q_2/q_1 q_2\} \Rightarrow$ (sono in numero di $n/q_1 q_2$ e quindi $|A_1 \cap A_2|=n/q_1 q_2$).

Analogamente si ha: $|A_1 \cap A_3|=n/q_1 q_3$ etc. e $|A_1 \cap A_2 \cap A_3|=n/q_1 q_2 q_3$ etc.

In conclusione, quindi:

$t=|A_1 \cup A_2 \cup \dots \cup A_r| = (n/q_1 + n/q_2 + \dots + n/q_r) - (n/q_1 q_2 + n/q_1 q_3 + \dots) + (n/q_1 q_2 q_3 + n/q_1 q_2 q_4 + \dots) + \dots \pm n/q_1 q_2 \dots q_r$ dove l'ultimo termine è positivo se r è dispari, negativo se r è pari.

Allora, per calcolare $\varphi(n)$:

$\varphi(n) = n - t = n - (n/q_1 + n/q_2 + \dots + n/q_r) + (n/q_1 q_2 + n/q_1 q_3 + \dots) - (n/q_1 q_2 q_3 + n/q_1 q_2 q_4 + \dots) + \dots \pm n/q_1 q_2 \dots q_r$

dove questa volta l'ultimo termine è positivo se r è pari, negativo se è dispari.

Operando alcune operazioni si può semplificare:

$\varphi(n) = n - t = n(1 - (1/q_1 + 1/q_2 + \dots + 1/q_r) + (1/q_1 q_2 + 1/q_1 q_3 + \dots) - (1/q_1 q_2 q_3 + 1/q_1 q_2 q_4 + \dots) + \dots \pm 1/q_1 q_2 \dots q_r) =$
 $= \text{premessa 2} = n(1 - 1/q_1)(1 - 1/q_2)(1 - 1/q_3) \dots (1 - 1/q_r) = n^* (q_1 - 1)/q_1^* (q_2 - 1)/q_2^* \dots (q_r - 1)/q_r^*.$

Ma $n = q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_r^{k_r}$ quindi, sostituendo:

$$\varphi(n) = q_1^{k_1-1} q_2^{k_2-1} q_3^{k_3-1} \dots q_r^{k_r-1} (q_1 - 1)(q_2 - 1) \dots (q_r - 1).$$

Esempio:

$\varphi(1000) = \varphi(2^{3*} 5^3) = 2^{2*} 5^2 (2-1)(5-1) = 400$, cioè i numeri compresi tra 1 e 1000 che sono coprimi con 1000 sono in numero di 400.

Lezione n°. 45 – 7 mar. 2001

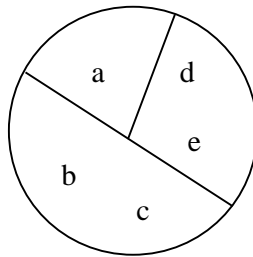
Partizioni di un insieme.

Se A è un insieme qualunque (non vuoto), un *partizione* di A è un insieme costituito da sottoinsiemi di A che sono non vuoti, a 2 a 2 disgiunti (senza elementi comuni, cioè con intersezione vuota) e la cui unione è tutto l'insieme A .

Esempi:

1. se R è una relazione di equivalenza in A , le sue classi di equivalenza formano una partizione di A .
2. se $A = \{a, b, c, d, e\}$, un esempio di partizione di A è: $\{\{a\}, \{b, c\}, \{d, e\}\}$.

Graficamente:



Se A è un insieme finito con n elementi e se m è un numero intero, con $1 \leq m \leq n$, quante sono le possibili partizioni di A in m sottoinsiemi? Il numero di tali partizioni si indica con $S(n, m)$ ed è detto **numero di Stirling**.

I casi limite sono:

- $m=1$: si ha una sola partizione di A in 1 sottoinsieme, cioè $\{A\}$, quindi $S(n, 1)=1$;
- $m=n$: si ha una sola partizione di A in n sottoinsiemi (se $|A|=n$) ed è quella in cui ogni elemento è "isolato" in un sottoinsieme, quindi $S(n, n)=1$.

Il problema è: in generale, quanto vale $S(n, m)$?

Proviamo a calcolare $S(n, m)$ per valori "piccoli" di n :

$S(1, 1)=1$; $S(2, 1)=1$; $S(2, 2)=1$; $S(3, 1)=1$; $S(3, 3)=1$; $S(4, 1)=1$; $S(4, 4)=1$ (sono i casi limite);

$S(3, 2)=3$, infatti, se $A = \{a, b, c\}$, le partizioni di A in 2 sottoinsiemi sono:

$\{\{a\}\{b, c\}\}$, $\{\{b\}\{a, c\}\}$, $\{\{c\}\{a, b\}\}$.

Già il calcolo di $S(4, 2)$ ed $S(4, 3)$ è più complicato.

Si possono distribuire questi numeri di Stirling in un triangolo, detto Triangolo di Stirling (in maniera simile a quanto fatto con il triangolo di Tartaglia):

			$S(1, 1)$		
		$S(2, 1)$		$S(2, 2)$	
	$S(3, 1)$		$S(3, 2)$		$S(3, 3)$
$S(4, 1)$		$S(4, 2)$		$S(4, 3)$	$S(4, 4)$
....

A differenza di quanto visto per il triangolo di Tartaglia, non esiste, in questo caso, una formula (funzione di n ed m) per calcolare il numero di Stirling generico. Esiste però una regola per determinare gli $S(n,m)$ di una riga del triangolo conoscendo quelli della riga precedente. La regola è la seguente:

$$S(n+1,m)=S(n,m-1)+m*S(n,m)$$

Quindi, per esempio, per calcolare gli elementi incogniti della quarta riga del triangolo di Stirling, si può applicare tale regola:

$$S(4,2)=S(3,1)+2*S(3,2)=1+2*3=7$$

$$S(4,3)=S(3,2)+3*S(3,3)=3+3*1=6$$

Esercizio: Calcolare la quinta riga del triangolo di Stirling.

$$\text{Svolgimento: } S(5,1)=S(5,5)=1.$$

$$S(5,2)=S(4,1)+2*S(4,2)=1+2*7=15$$

$$S(5,3)=S(4,2)+3*S(4,3)=7+3*6=25$$

$$S(5,4)=S(4,3)+4*S(4,4)=6+4*1=10$$

Dimostrazione della regola $S(n+1,m)=S(n,m-1)+m*S(n,m)$.

Sia A un insieme di $n+1$ elementi: $A=\{a_1,a_2,a_3,\dots,a_n,a_{n+1}\}$; $S(n+1,m)$ è il numero di partizioni di A in m sottoinsiemi. Suddividiamo tali possibili partizioni in 2 *categorie*:

categoria 1: le partizioni di A in m sottoinsiemi in cui un elemento (ad esempio l'elemento a_{n+1}) è da solo in un sottoinsieme;

categoria 2: le partizioni di A in m sottoinsiemi in cui lo stesso elemento (a_{n+1}) è insieme ad altri in un sottoinsieme.

Per calcolare $S(n+1,m)$ basta sommare il numero di partizioni delle due categorie.

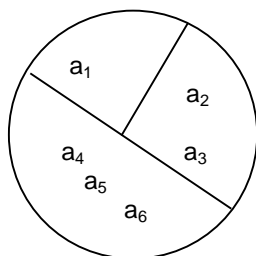
Contiamo allora le partizioni della prima categoria: togliendo a_{n+1} , si ottiene una partizione dell'insieme $\{a_1,a_2,\dots,a_n\}$ in $(m-1)$ sottoinsiemi (abbiamo “cancellato” l'elemento a_{n+1} ed il sottoinsieme da esso costituito). Quindi tali partizioni sono in numero di $S(n,m-1)$.

Contiamo adesso le partizioni della seconda categoria: togliendo a_{n+1} si ottiene una partizione dell'insieme $\{a_1,a_2,\dots,a_n\}$ in m sottoinsiemi (abbiamo “cancellato” l'elemento a_{n+1} ma non il sottoinsieme che lo conteneva) e tali partizioni sono in numero di $S(n,m)$.

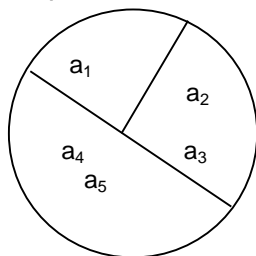
Ma ogni partizione di $\{a_1,a_2,\dots,a_n\}$ in m sottoinsiemi, non determina una sola partizione della seconda categoria, perché a_{n+1} si può *inserire* in m modi diversi (in ciascuno degli m sottoinsiemi) e quindi, in totale, il numero di partizioni della seconda categoria è $m*S(n,m)$.

Esempio:

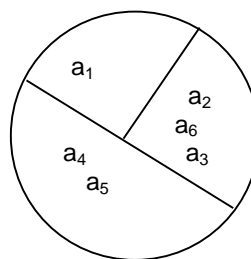
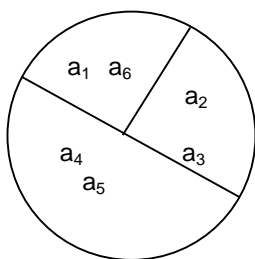
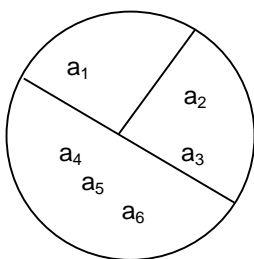
se $n=5$ ed $m=3$, $A=\{a_1, a_2, a_3, a_4, a_5, a_6\}$ ($|A|=n+1=6$). Presa, per esempio, una partizione della seconda categoria (partizione di A in 3 sottoinsiemi in cui a_6 compare con altri elementi in un sottoinsieme) avremo, graficamente:



“cancellando” a_6 , si ottiene una partizione di $\{a_1, a_2, a_3, a_4, a_5\}$ in 3 sottoinsiemi:



Ma quest’ultima partizione (con il processo inverso di aggiungere a_6 a qualche sottoinsieme) determina in tutto 3 partizioni della seconda categoria:



Quindi, ricapitolando, si ha che:

$$S(n+1) = \underset{(1^{\text{a}} \text{ categoria})}{S(n, m-1)} + \underset{(2^{\text{a}} \text{ categoria})}{m \cdot S(n, m)}$$

e la regola è dimostrata.

Il numero di Stirling è importante perché serve per calcolare, dati due insiemi finiti A e B , rispettivamente di ordine n ed m , se $n \geq m$, il numero di applicazioni surgettiva $f: A \rightarrow B$ (tale numero risulterà uguale a $m! \cdot S(n, m)$).

Lezione n°. 46 – 9 mar. 2001

Numero delle applicazioni surgettive fra insiemi finiti.

Siano A e B due insiemi finiti di ordine, rispettivamente, n ed m. Contiamo le applicazioni surgettive $f:A \rightarrow B$. Supponiamo $n \geq m$ (se fosse $n < m$ non ci sarebbero applicazioni surgettive da A a B).

Esempio:

$A=\{a,b,c,d,e\}$, $B=\{r,s,t\}$, $|A|=5$, $|B|=3$.

Per costruire una $f:A \rightarrow B$ surgettiva, dobbiamo scegliere quali elementi di A hanno immagine r, quali s e quali t. Una tale scelta equivale ad una partizione di A in 3 sottoinsiemi; ad esempio si potrebbe scegliere $(a,b) \rightarrow r$, $c \rightarrow s$ e $(d,e) \rightarrow t$, ottenendo quindi la partizione $\{\{a,b\}, \{c\}, \{d,e\}\}$. Il numero totale di partizioni è $S(5,3)$ (numero di Stirling). Ma la partizione di A che costruiamo non determina una sola applicazione surgettiva: ad esempio, la partizione precedente $\{\{a,b\}, \{c\}, \{d,e\}\}$ determina 6 diverse applicazioni surgettive (sono $6=3!$ perché è il numero delle disposizioni semplici dei tre elementi r,s,t presi a 3 a 3):

1. $(a,b) \rightarrow r$, $c \rightarrow s$ e $(d,e) \rightarrow t$;
2. $(a,b) \rightarrow s$, $c \rightarrow t$ e $(d,e) \rightarrow r$;
3. $(a,b) \rightarrow t$, $c \rightarrow r$ e $(d,e) \rightarrow s$;
4. $(a,b) \rightarrow r$, $c \rightarrow t$ e $(d,e) \rightarrow s$;
5. $(a,b) \rightarrow s$, $c \rightarrow r$ e $(d,e) \rightarrow t$;
6. $(a,b) \rightarrow t$, $c \rightarrow s$ e $(d,e) \rightarrow r$;

quindi il numero totale di applicazioni surgettive $f:A \rightarrow B$ è uguale a $3! \cdot S(5,3)$.

In generale, se $|A|=n$ e $|B|=m$, il numero di applicazioni surgettive $f:A \rightarrow B$ è uguale a $m! \cdot S(n,m)$.

Disegni.

Supponiamo che un industria produca v **varietà** di uno stesso prodotto (v è un intero ≥ 1) e voglia sottoporre tali varietà ad un test di qualità: vi saranno delle persone (**testers**) che effettueranno i test. Perché il test sia equilibrato ed omogeneo nei risultati, è opportuno che:

1. ogni tester testi un numero k di varietà fra le v disponibili, con k uguale per tutti i testers;
2. ognuna di tali varietà sia testata dallo stesso numero r di testers.

Esempio:

sia $v=6$, $k=3$, $r=2$ (in totale 6 varietà, ogni tester ne testa 3 ed ogni varietà viene testata da 2 testers). È possibile, con questi dati, effettuare il test? E con quanti testers? Con i dati precedenti la risposta è positiva; infatti, se l'insieme delle 6 varietà è $A=\{a,b,c,d,e,f\}$ si possono impiegare 4 testers con lo schema seguente:

1° tester: $\{a,b,c\}$

2° tester: $\{b,c,d\}$

3° tester: $\{d,e,f\}$

4° tester: $\{e,f,a\}$.

Domanda *generale*: dati v,k,r generici, è possibile sempre effettuare il test? E con quanti testers?

Generalizzando il problema: si chiama **disegno di parametri** (v,k,r) una struttura formata da:

1. un insieme A di ordine v (insieme delle **varietà**);
2. alcuni sottoinsiemi non vuoti di A (detti **blocchi del disegno**), tutti dello stesso ordine k e tali che ogni elemento di A appartiene esattamente ad r di tali blocchi.

In pratica i blocchi sono i testers.

Problema: quali condizioni si devono imporre nei parametri (v,k,r) affinché il disegno si possa costruire? E quanti sono i blocchi necessari?

Sia dato l'insieme $A=\{a_1,a_2,\dots,a_v\}$ e si supponga che si possa costruire il disegno di parametri (v,k,r) con esattamente x blocchi; gli x blocchi B_1,B_2,\dots,B_x saranno dei sottoinsiemi di A tutti di ordine k ; ma il numero totale di sottoinsiemi di un insieme di ordine

v che hanno ordine k è uguale alle combinazioni semplici di v elementi presi a k a k , cioè è uguale a $\binom{v}{k}$ e quindi una condizione è che sia $x \leq \binom{v}{k}$.

Inoltre si può definire una relazione R dall'insieme A all'insieme dei blocchi $\{B_1, B_2, \dots, B_x\}$ dicendo che un elemento $a_i \in A$ è in relazione con un blocco B_j quando $a_i \in B_j$. Se rappresentiamo tale relazione in forma matriciale:

	B_1	B_j	B_x
a_1							
...							
a_i							
...							
...							
a_v							

Si avranno v righe ed x colonne; nella casella generica ci sarà un valore 1 se $a_i \in B_j$, 0 se $a_i \notin B_j$.

Il fatto che ogni blocco abbia ordine k dice che ogni colonna contiene esattamente k valori uguali ad 1. Il fatto che ogni elemento a_i compare esattamente in r blocchi, dice che ogni riga contiene r valori uguali ad 1. Contando per righe e per colonne il numero di 1 nella matrice, si ha:

$v \cdot r = x \cdot k$ quindi $x = v \cdot r / k$ (il numero di blocchi è "obbligato" e coincide con $v \cdot r / k$, e poiché x deve essere un numero intero, si deve avere che k sia divisore di $v \cdot r$).

Allora, se il disegno di parametri (v, k, r) si può costruire è certo che sono verificate le due seguenti condizioni:

$$1) \ k \text{ divisore di } v \cdot r \quad \text{e} \quad 2) \ x = \frac{v \cdot r}{k} \leq \binom{v}{k}$$

Esempio:

un disegno di parametri $(10, 7, 4)$ non si può costruire perché 7 non è divisore di $10 \cdot 4 = 40$.

Un risultato interessante è che, viceversa, se le due condizioni sono verificate, allora si può costruire un disegno di parametri (v, k, r) .

Lezione n°. 47 – 12 mar. 2001

Se sono verificate le due seguenti condizioni:

$$1) \ k \text{ divisore di } v \cdot r \quad \text{e} \quad 2) \ x = \frac{v \cdot r}{k} \leq \binom{v}{k}$$

allora si può costruire un disegno di parametri (v, k, r) .

Dimostrazione:

supponiamo vere le due condizioni e sia dato l'insieme $A = \{a_1, a_2, \dots, a_v\}$, di ordine v . Lo scopo è la *costruzione* dei blocchi (cioè dei sottoinsiemi di A di ordine k tali che ogni elemento di A sia in r blocchi). Sappiamo che il numero dei blocchi sarà uguale a $x = v \cdot r / k$ (e che tale numero è un intero, per la prima condizione). Inizialmente, scegliamo, a piacere, x sottoinsiemi di A : B_1, B_2, \dots, B_x , tutti di ordine k (il fatto che tale scelta si possa fare

è dovuto alla seconda condizione; il numero totale di sottoinsiemi di ordine k è $\binom{v}{k}$ e tale

numero è $\geq x$). Se ogni elemento dell'insieme A compare esattamente in r blocchi, abbiamo già trovato il disegno cercato, Se così non è, si procede con delle modifiche dei blocchi "per aggiustamenti successivi". Definiamo una relazione dall'insieme A all'insieme dei blocchi $\{B_1, B_2, \dots, B_x\}$ definendo un elemento generico $a_i \in A$ associato ad un blocco B_j quando $a_i \in B_j$. Rappresentiamo tale relazione in forma matriciale:

	B_1	B_j	B_x
a_1							
...							
a_i							
...							
...							
a_v							

In ogni colonna ci sono k valori uguali ad 1 (ogni blocco ha ordine k) e quindi, contando per colonne, nella matrice, in totale vi sono $k \cdot x$ valori uguali a 1. In ogni riga, il numero di valori uguali ad 1 corrisponde al numero di blocchi a cui appartiene l'elemento della riga. Se il disegno non è ancora costruito, vuol dire che non tutte le righe conterranno esattamente r valori uguali a 1. Ma non tutte le righe "errate" (cioè con un numero di valori 1 diverso da r) possono avere un numero di valori 1 superiore ad r , perché in questo caso il numero totale di valori 1 nella matrice sarebbe $> v \cdot r = x \cdot k$, e ciò sarebbe assurdo perché il numero totale di valori 1 nella matrice è $x \cdot k$. Con un ragionamento simile si dimostra che non tutte le righe ("errate") possono avere un numero di valori 1 inferiore ad r . Allora vi

sarà almeno una riga i con un numero r_i di valori 1 e con $r_i > r$ (in eccesso) ed almeno una riga j con un numero r_j di valori 1 e con $r_j < r$ (in difetto).

Si avrà una situazione simile:

	B_1	...	B_j	...	B_x	
a_1						
...						
a_i						r_i valori uguali a 1
...						
a_j						r_j valori uguali a 1
...						
a_v						

$$\left. \begin{array}{l} r_i \text{ valori uguali a 1} \\ r_j \text{ valori uguali a 1} \end{array} \right\} r_j < r < r_i$$

La riga i ha un numero di valori 1 superiore a quello della riga j , quindi non può avvenire che “sotto” i valori 1 della riga i (nella stessa colonna) vi sia sempre un valore 1 nella riga j . Vi è almeno un valore 1 (in realtà almeno 2) nella riga i che ha “al di sotto” (nella stessa colonna) un valore 0 nella riga j .

	B_1	...	B_s	...	B_x	
a_1						
...						
a_i			1			
...						
a_j			0			
...						
a_v						

Si scambiano allora un tale valore 0 ed un tale valore 1 tra loro (in pratica, dal punto di vista dell'insiemistica, si cambia il blocco B_s introducendo l'elemento a_j e togliendo l'elemento a_i , non alterando l'ordine k del blocco).

Ripetendo tale “aggiustamento” più volte si ottiene il disegno voluto (cioè tutte le righe hanno r valori uguali a 1).

Osservazione: il disegno ottenuto non è unico, vista l'arbitrarietà di alcune scelte.

Esempio: costruire un disegno di parametri $(5,3,3)$.

Anzitutto si verificano le due condizioni: 3 è divisore di $5 \cdot 3$ e $x = 5 \cdot 3 / 3 = 5 < \binom{5}{3} = 10$

Si prende quindi un insieme di ordine 5, $A = \{a, b, c, d, e\}$. Il numero di blocchi sarà 5 (tutti di ordine 3). Si scelgono arbitrariamente 5 sottoinsiemi di A , ognuno di ordine 3;

$B_1 = \{a, b, c\}$, $B_2 = \{b, c, d\}$, $B_3 = \{c, d, e\}$, $B_4 = \{a, b, d\}$, $B_5 = \{b, d, e\}$.

Si costruisce la matrice della relazione da A in $\{B_1, B_2, B_3, B_4, B_5\}$:

	B ₁	B ₂	B ₃	B ₄	B ₅
a	1	0	0	1	0
b	1	1	0	1	1
c	1	1	1	0	0
d	0	1	1	1	1
e	0	0	1	0	1

In ogni riga devono esserci 3 valori uguali a 1; la riga 3 va bene; le righe 2 e 4 sono “in eccesso” (4 valori 1) e le righe 1 e 5 sono “in difetto” (2 valori 1). “Aggiustiamo” le righe 4 e 5: considerando la colonna 4 si scambiano i valori 1 e 0 nelle righe 4 e 5 (cioè si introduce l’elemento e in B₄ e si toglie l’elemento d). Poi si “aggiustano” le righe 1 e 2, considerando la colonna 2 e scambiando i valori 1 e 0 (nel blocco B₂ si toglie b e si introduce a). Si ottiene quindi la matrice “corretta”:

	B ₁	B ₂	B ₃	B ₄	B ₅
a	1	1	0	1	0
b	1	0	0	1	1
c	1	1	1	0	0
d	0	1	1	0	1
e	0	0	1	1	1

I blocchi sono allora: $B_1=\{a,b,c\}$, $B_2=\{a,c,d\}$, $B_3=\{c,d,e\}$, $B_4=\{a,b,e\}$, $B_5=\{b,d,e\}$.

NOTA: nella scelta di modifica dei blocchi bisogna evitare di creare due o più blocchi uguali.

Esercizio: costruire un disegno di parametri (8,4,3).

Svolgimento: verifico che le condizioni siano vere:

$$4 \text{ è divisore di } 8 \cdot 3 = 24 \text{ e } x = 8 \cdot 3 / 4 = 6 < \binom{8}{4} = 70$$

Considero un insieme di ordine 8, $A=\{a,b,c,d,e,f,g,h\}$. Il numero di blocchi sarà 6 (tutti di ordine 3). Scelgo arbitrariamente 6 sottoinsiemi di A, ognuno di ordine 4;

$B_1=\{a,b,c,d\}$, $B_2=\{b,c,d,e\}$, $B_3=\{c,d,e,f\}$, $B_4=\{a,f,g,h\}$, $B_5=\{b,d,e,g\}$, $B_6=\{e,f,g,h\}$.

Costruisco la matrice della relazione da A in $\{B_1, B_2, B_3, B_4, B_5, B_6\}$:

	B ₁	B ₂	B ₃	B ₄	B ₅	B ₆
a	1	0	0	1	0	0
b	1	1	0	0	1	0
c	1	1	1	0	0	0
d	1	1	1	0	1	0
e	0	1	1	0	1	1
f	0	0	1	1	0	1
g	0	0	0	1	1	1
h	0	0	0	1	0	1

In ogni riga devono esserci 3 valori uguali a 1; le righe 2,3,6 e 7 vanno bene; le righe 4 e 5 sono “in eccesso” (4 valori 1) e le righe 1 e 8 sono “in difetto” (2 valori 1). “Aggiusto” le

righe 1 e 4: considerando la colonna 2 scambio i valori 1 e 0 nelle righe 1 e 4 (cioè si introduce l'elemento a in B_2 e si toglie l'elemento d). Poi "aggiusto" le righe 5 e 8: considerando la colonna 5 scambiando 1 e 0 (nel blocco B_5 si toglie e e si introduce h). Ottengo così la seguente matrice "corretta" ed i blocchi che ne conseguono:

	B_1	B_2	B_4	B_4	B_5	B_6	
a	1	1	0	1	0	0	$B_1=\{a,b,c,d\}$
b	1	1	0	0	1	0	$B_2=\{a,b,c,e\}$
c	1	1	1	0	0	0	$B_3=\{c,d,e,f\}$
d	1	0	1	0	1	0	$B_4=\{a,f,g,h\}$
e	0	1	1	0	0	1	$B_5=\{b,d,g,h\}$
f	0	0	1	1	0	1	$B_6=\{e,f,g,h\}$
g	0	0	0	1	1	1	
h	0	0	0	1	1	1	

Lezione n°. 48 – 14 mar. 2001

2-disegni.

Siano date v squadre sportive e si vogliano organizzare dei tornei che coinvolgano, ognuno, k delle v squadre (con k uguale per tutti i tornei), ed in modo che ogni squadra incontri ogni altra in un numero r_1 di tornei (con r_1 uguale per tutte le squadre).

Esempio: se $v=7$, $k=3$, $r_1=1$: vi dovrebbero essere 7 squadre, 3 squadre per ogni torneo ed ogni squadra dovrebbe incontrare ogni altra esattamente in un torneo. Si può realizzare un tale progetto? Se l'insieme delle squadre è $A=\{a,b,c,d,e,f,g\}$ si possono organizzare i seguenti tornei:

$B_1=\{a,b,c\}$, $B_2=\{e,b,c\}$, $B_3=\{e,f,a\}$, $B_4=\{f,g,c\}$, $B_5=\{e,g,b\}$, $B_6=\{d,g,a\}$, $B_7=\{f,d,b\}$.

(7 tornei, ogni torneo ha 3 squadre, ogni coppia di squadre è presente esattamente in un torneo).

Formalizzando il problema: si chiama **2-disegno di parametri (v,k,r_1)** una struttura formata da:

1. un insieme A di ordine v ;
2. dei sottoinsiemi di A (detti **blocchi**), ognuno di ordine k e tali che ogni coppia di elementi compaia esattamente in r_1 dei sottoinsiemi.

Osservazione: invece, nel concetto di disegno, si pretende che ogni singolo elemento di A compaia un numero costante r di blocchi.

In pratica, quello costruito nell'esempio è un 2-disegno di parametri $(7,3,1)$; ma si nota anche, nell'esempio, che ogni elemento di A compare esattamente in 3 blocchi e, quindi, il

2-disegno costruito è anche un disegno di parametri (7,3,3). Questo fatto non è casuale, ma vale sempre. Esiste il seguente

Teorema: ogni 2-disegno di parametri (v,k,r_1) è sempre anche un disegno di parametri (v,k,r) , dove $r=r_1*(v-1)/(k-1)$.

[nell'esempio precedente $r=1*(7-1)/(3-1)=3$].

Dimostrazione: la tesi è: ogni singolo elemento di A dovrebbe comparire esattamente in r blocchi, dove $r=r_1*(v-1)/(k-1)$.

Sia $A=\{a_1,a_2,\dots,a_v\}$ e ragioniamo sull'elemento a_1 (il ragionamento sugli altri elementi è simile). Consideriamo i blocchi che contengono a_1 : siano essi B_1,B_2,\dots,B_x (la tesi è proprio che il numero di tali blocchi sia $x=r=r_1*(v-1)/(k-1)$).

Consideriamo l'insieme $A-\{a_1\}=\{a_2,a_3,\dots,a_v\}$ e la relazione R dall'insieme $A-\{a_1\}$ all'insieme dei blocchi $\{B_1,B_2,\dots,B_x\}$ dove $a_i R B_j$ se $a_i \in B_j$. La rappresentazione matriciale comprende $(v-1)$ righe ed x colonne:

	B_1	B_2	B_x
a_2						
a_3						
...						
...						
a_v						

Contiamo i valori 1 per colonne: ogni blocco fra B_1,B_2,\dots,B_x contiene esattamente k elementi, ma poiché ognuno di tali blocchi contiene a_1 , ogni blocco contiene $(k-1)$ tra gli elementi a_2, a_3,\dots,a_v e quindi in ogni colonna della matrice vi sono $(k-1)$ valori 1 ed in totale, nella matrice, i valori 1 sono $x*(k-1)$.

Contiamo ora i valori 1 per righe: nella 1^a riga, ad esempio, il numero di valori 1 è uguale al numero di blocchi (fra B_1,B_2,\dots,B_x) che contengono a_2 , ma tali blocchi sono quelli che, contemporaneamente, contengono a_1 , quindi il numero di valori 1 nella 1^a riga è uguale al numero di blocchi del 2-disegno che contengono la coppia a_1,a_2 e tale numero è r_1 , per cui nella 1^a riga vi sono r_1 valori uguali a 1. Analogamente nelle altre righe ed in totale, nella matrice, il numero di valori 1 è $r_1*(v-1)$.

Eguagliando i due risultati ottenuti, si ha:

$x*(k-1)=r_1*(v-1) \Rightarrow x=r_1*(v-1)/(k-1)$, cioè la tesi.

Osservazione: il teorema non si può invertire, perché vi sono dei disegni che non sono 2-disegni (un caso è l'esempio fatto per i "test di qualità", disegno di parametri (6,3,2), in cui vi sono delle coppie di elementi che non compaiono in nessun blocco).

Conseguenza importante del teorema: se è possibile costruire un 2-disegno di parametri (v, k, r_1) , poiché esso è anche un disegno di parametri $(v, k, r_1^*(v-1)/(k-1))$, dovendo essere $r_1^*(v-1)/(k-1)$ un numero intero, si ha che:

- $(k-1)$ deve essere divisore di $r_1^*(v-1)$;

Inoltre, per le condizioni che conosciamo sui disegni, si deve avere anche che:

- k deve essere divisore di $v^*r = v^*r_1(v-1)/(k-1)$;

$$- \frac{v^*r}{k} = v^* \frac{r_1(v-1)}{k(k-1)} \leq \binom{v}{k}$$

Ma, se sono vere le 3 condizioni precedenti **non è detto** che si possa costruire il 2-disegno (può esistere oppure no).

Problema aperto: trovare delle condizioni necessarie e sufficienti su v, k, r_1 che assicurino l'esistenza del 2-disegno.

Lezione n°. 49 – 16 mar. 2001

Piano proiettivo.

Sappiamo che un 2-disegno di parametri (v, k, r_1) è una struttura formata da:

1. un insieme A di ordine v ;
2. dei sottoinsiemi di A (detti blocchi), ognuno di ordine k e tali che ogni coppia di elementi di A compaia esattamente in r_1 dei sottoinsiemi.

Sappiamo anche che un tale 2-disegno è automaticamente anche un disegno di parametri (v, k, r) , dove $r = r_1(v-1)/(k-1)$ (r è il numero di blocchi che contiene ogni singolo elemento di A).

Un 2-disegno è detto **piano proiettivo** se $r_1 = 1$ (ogni coppia di elementi compare esattamente in un blocco), e se due blocchi diversi hanno sempre in comune un solo elemento.

I blocchi di un piano proiettivo sono detti anche **rette** (per ricordare che la situazione è simile a quella delle rette nel piano: per due punti passa una sola retta, e due rette incidenti hanno in comune un solo punto).

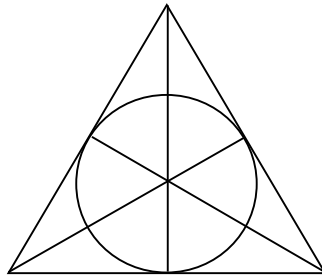
Ammettiamo di avere un piano proiettivo di parametri $(v, k, 1)$ (v è il numero dei “punti”, k il numero di “punti” che vi è in ogni retta); quanti sono i blocchi (le rette)?

Sappiamo che tale piano proiettivo, essendo un 2-disegno, è anche un disegno di parametri $(v, k, \frac{v-1}{k-1})$ e il numero di blocchi è $x = \frac{v(v-1)}{k(k-1)}$ (perché $x = v^*r/k$).

Esempio:

costruiamo un piano proiettivo di parametri (7,3,1) (quindi: 7 punti in totale, ogni blocco (retta) contiene 3 punti, ogni coppia di punti compare in un solo blocco e due blocchi hanno in comune un solo punto).

Si può usare una costruzione geometrica: si prende un triangolo equilatero, il cerchio inscritto e le mediane:



Come punti si prendono: i 3 vertici più i punti medi dei lati più il centro del cerchio; come blocchi (rette) si prendono i 3 lati del triangolo, più le 3 mediane più la circonferenza. Si nota che, nell'esempio precedente, i parametri k ed r (k =numero di punti su ogni blocco ed r =in quanti blocchi compare un singolo punto) sono uguali (entrambi pari a 3). Questo non è un fatto casuale:

teorema: in ogni piano proiettivo di parametri $(v,k,1)$ (pensandolo come un disegno di parametri (v,k,r)) si ha sempre $k=r$.

Dimostrazione: sia x un "punto" a caso dell'insieme A ; esso è contenuto esattamente in r blocchi B_1, B_2, \dots, B_r (blocchi che contengono x). Fissiamo poi un blocco B che non contenga x : esso è di ordine k .

$$B = \{x_1, x_2, \dots, x_k\} \text{ (con } x_1, x_2, \dots, x_k \text{ tutti diversi da } x)$$

Definiamo un'applicazione $\varphi: B = \{x_1, x_2, \dots, x_k\} \rightarrow \{B_1, B_2, \dots, B_r\}$, dimostriamo che essa è biunivoca ed avremo la tesi (infatti due insiemi finiti fra i quali vi è un'applicazione biunivoca hanno lo stesso ordine $\Rightarrow k=r$).

Definiamo φ : prendiamo un elemento $x_i \in B$; la coppia di punti x, x_i compare esattamente in un blocco (per definizione di piano proiettivo) che è uno dei blocchi B_1, B_2, \dots, B_r (perché sono tutti quelli che contengono x). Definiamo proprio $\varphi(x_i)$ =quell'unico blocco B_j che contiene la coppia x, x_i .

φ è iniettiva: se $x_i \neq x_s$ in B la tesi è $\varphi(x_i) \neq \varphi(x_s)$; ora, se, per assurdo, fosse $\varphi(x_i) = \varphi(x_s)$, ricordando che:

$$\varphi(x_i) = \text{unico blocco } B_j \text{ che contiene la coppia } x, x_i;$$

$$\varphi(x_s) = \text{unico blocco } B_t \text{ che contiene la coppia } x, x_s;$$

si avrebbe che $B_j=B_t$ ed il blocco $B_j=B_t$ avrebbe in comune con il blocco B i punti x_i, x_s e ciò è impossibile perché 2 blocchi hanno in comune un solo punto).

φ è surgettiva: preso un elemento B_c del codominio (quindi B_c è uno dei blocchi B_1, B_2, \dots, B_r che contengono x) la tesi consiste nel trovare un elemento $x_i \in B$ tale che $\varphi(x_i) =$ unico blocco B_c ; ma i due blocchi B e B_c hanno (per definizione di piano proiettivo) un solo punto in comune: chiamiamo tale punto x_i (è un punto sia in B che in B_c). Ma $\varphi(x_i)$ è quell'unico blocco che contiene x, x_i , cioè B_c . Il teorema è così dimostrato (φ iniettiva e surgettiva \Rightarrow biunivoca).

Conseguenze del teorema: in un piano proiettivo di parametri $(v, k, 1)$ i due parametri k ed r sono uguali; ma $r = \frac{v-1}{k-1}$ quindi $k = \frac{v-1}{k-1} \Rightarrow k(k-1) = v-1$.

Il numero $k-1$ lo indichiamo con n , ed è detto **grado del piano proiettivo**: $k-1=n$; tutti i parametri del piano proiettivo si possono scrivere in funzione di n , infatti:

$$k=n+1;$$

$$v=k(k-1)+1=(n+1)n+1=n^2+n+1.$$

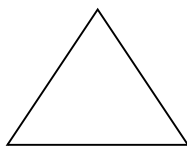
Quindi, in totale, il piano proiettivo è:

1. un 2-disegno di parametri $\left(\begin{matrix} n^2+n+1, n+1, 1 \\ v, k, r \end{matrix} \right);$
2. un disegno di parametri $\left(\begin{matrix} n^2+n+1, n+1, 1 \\ v, k, r=k \end{matrix} \right).$

Problema: per quali valori del grado n si riesce a costruire un piano proiettivo?

Per $n=2$ abbiamo costruito l'esempio del triangolo;

per $n=1$ è pure possibile, considerando un triangolo (3 punti in tutto (i vertici), i blocchi sono i lati del triangolo):



Un po' di storia.

Si costruiscono facilmente piani proiettivi di grado 3,4 e 5. Non si riusciva invece a costruire un piano proiettivo di grado 6 finché, nel 1938, il matematico Bose scoprì un collegamento tra tale problema ed un classico problema di Eulero.

Problema dei 36 ufficiali di Eulero e i quadrati latini (periodo: fine '700).

Il problema è il seguente: dati 36 ufficiali, ognuno appartenente ad una tra 6 armi diverse, ed ognuno avente un grado diverso fra 6 possibili (in tutte le combinazioni possibili arma-grado). Si vogliono disporre i 36 ufficiali in un quadrato di 6 righe e 6 colonne, in modo che in nessuna riga e nessuna colonna si presentino ufficiali appartenenti alla stessa arma o con lo stesso grado. È possibile?

Formalizziamo il problema: affrontiamo, come esempio, il caso di 9 ufficiali (3 armi e 3 gradi); codifichiamo le armi con i numeri 1,2,3 e allo stesso modo codifichiamo i gradi con i numeri 1,2,3 ed identifichiamo ogni ufficiale con due numeri (il primo indicante l'arma ed il secondo il grado). In questo caso il problema ha soluzione, per esempio:

11	22	33
23	31	12
32	13	21

Tale quadrato si può pensare come risultante dalla sovrapposizione di due quadrati "singoli", ottenuti *isolando* l'arma nel primo ed il grado nel secondo:

1	2	3
2	3	1
3	1	2

arma

1	2	3
3	1	2
2	3	1

grado

Si definisce **quadrato latino di dimensione n** un quadrato di n righe ed n colonne tale che in ogni riga ed ogni colonna vi siano i numeri interi da 1 ad n , senza ripetizioni, sia sulle righe che sulle colonne.

Due quadrati latini si dicono **ortogonali tra loro** se, sovrapponendoli (cioè costruendo un terzo quadrato le cui caselle contengano le coppie ordinate di numeri tratti dai due quadrati) si ottenga un quadrato che, nelle n^2 caselle contenga tutte le possibili coppie ordinate di numeri da 1 ad n .

Il problema di Eulero chiede quindi la costruzione di due quadrati latini ortogonali di dimensione 6. È possibile?

Il matematico Tarry (nel 1900) elencò tutti i possibili quadrati latini di dimensione 6 e verificò che non ve ne erano 2 ortogonali fra loro: quindi la risposta al problema dei 36 ufficiali è negativa.

Eulero aveva congetturato che il problema dei quadrati latini ortogonali non avesse soluzione ne' per dimensione uguale a 6, ne' per dimensioni uguali a 10, 14, 18, ... (6+un multiplo di 4), ma si sbagliava. Nel 1960, infatti, si dimostrò che solo per $n=6$ non si potevano costruire due quadrati latini ortogonali di dimensione n .

Inoltre si dimostrò che un piano proiettivo di grado n si può costruire se e solo se si possono costruire $n-1$ quadrati latini di dimensione n tutti a coppie ortogonali (questo vale per ogni $n \geq 3$). Quindi, per esempio:

1. se si vuole costruire un piano proiettivo di grado $n=3$, basta costruire 2 quadrati latini di dimensione 3 ortogonali tra loro;
2. se si vuole costruire un piano proiettivo di grado $n=4$, basta costruire 3 quadrati latini di dimensione 4 a 2 a 2 ortogonali fra loro;
3. etc.

Questo spiega perché non esiste un piano proiettivo di grado 6: non esistono 2 quadrati latini di dimensione 6 ortogonali tra loro (ne servirebbero addirittura cinque!).

La situazione attuale delle ricerche sui piani proiettivi è la seguente:

si è dimostrato che un piano proiettivo si può sempre costruire quando il grado n è un numero primo o una potenza di un numero primo, quindi:

n:	2	3	$4=2^2$	5	6	7	$8=2^3$	$9=3^2$	10	11	12	...
	ok	ok	ok	ok	no	ok	ok	ok	? (no)	ok	?	...

Il caso $n=10$ fu risolto, in senso negativo, solo nel 1988 (dal matematico Lam, con oltre 2000 ore di lavoro di un potentissimo computer!).

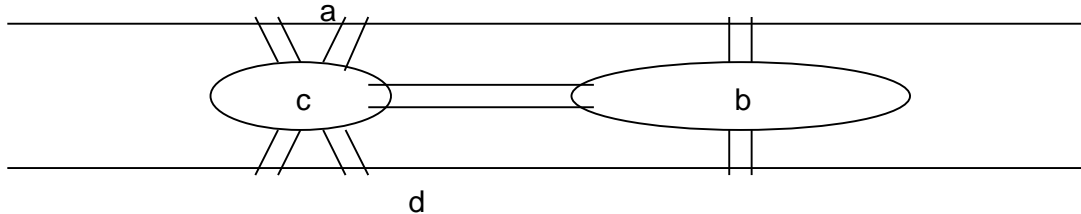
Per $n=12$ ancora non è noto!

Lezione n°. 51 – 21 mar. 2001

Teoria dei grafi.

Origine storica: problema dei ponti di Könisberg (Eulero, 1736).

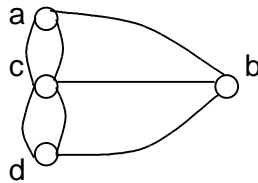
Il problema posto era relativo al fiume Pregel attraversato da 7 ponti che collegavano 4 zone di terra:



a,b,c,d sono le zone di terra.

Si voleva sapere se fosse possibile partire da una delle zone di terra, percorrere tutti i 7 ponti una ed una sola volta e tornare al punto di partenza.

Formalizzando il problema, si rappresentano le zone di terra a,b,c,d come punti nel piano ed i ponti come “archi” che li uniscono:



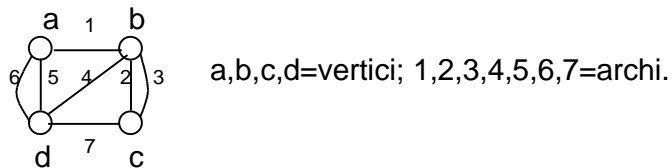
Tale tipo di struttura è detto **grafo (non orientato)**. In una tale struttura si distinguono i **vertici** (i punti del piano) e gli **archi** che uniscono alcuni dei vertici (è permesso che tra 2 vertici esistano più archi o che non ne esista nessuno). È anche possibile che vi sia qualche arco (detto **cappio**) che unisce un vertice con se stesso.



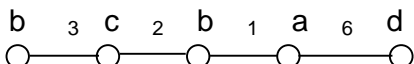
In generale si considereranno grafi senza cappi.

Dato un grafo si definisce **cammino nel grafo** una successione di archi tali che ognuno abbia in comune con il successivo un vertice.

Esempio: se il grafo è il seguente



un esempio di cammino può essere il seguente:



Cammino Euleriano.

In un grafo si chiama **cammino Euleriano** un cammino che percorre tutti gli archi del grafo, ognuno una ed una sola volta; un tale cammino è detto **ciclico** se il vertice di *partenza* coincide con quello di *arrivo*.

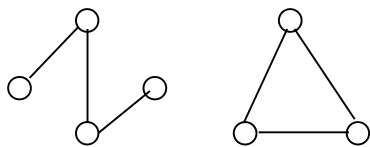
Il problema dei ponti, dal punto di vista dei grafi, diventa: esiste o no, nel grafo corrispondente, un cammino Euleriano ciclico?

Il problema generale è: dato un grafo, sotto quali condizioni esiste in esso un cammino Euleriano ciclico?

Introduciamo alcune nozioni preliminari:

1. **Grafo connesso:** si chiama grafo connesso un grafo in cui, comunque presi due vertici distinti, esiste sempre un cammino che li unisce (anche ridotto ad un solo arco). Il grafo dell'esempio precedente, così come quello relativo ai ponti, è connesso.

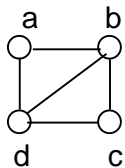
Un esempio di grafo non connesso può essere il seguente:



vi sono delle coppie di vertici non raggiungibili uno dall'altro con un cammino.

2. **grado di un vertice:** è, per definizione, il numero di archi che incidono su tale vertice (se l'arco è un cappio viene contato 2 volte).

Esempio:



il grado di a è 2, il grado di b è 3, etc.

un vertice è detto **isolato** se ha grado 0 (non vi sono archi che incidono in esso).

Teorema di Eulero.

Sia dato un grafo privo di vertici isolato. Allora: esiste nel grafo un cammino Euleriano ciclico se e solo se il grafo è connesso ed il grado di tutti i vertici è pari.

(ad esempio, nel grafo relativo ai ponti di Königsberg tutti i vertici hanno grado dispari e quindi il problema ha soluzione negativa).

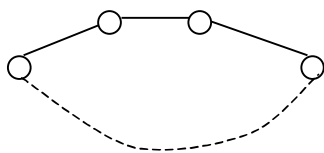
Dimostrazione.

Prima implicazione:

Ipotesi: esiste un cammino ciclico Euleriano;

tesi: è un grafo connesso con vertici tutti di grado pari.

Rappresentiamo un tale cammino (Euleriano ciclico):



In tale rappresentazione compaiono tutti gli archi del grafo, ognuno una ed una sola volta (i vertici possono anche essere ripetuti). Poiché, per ipotesi, non esistono vertici isolati, nella rappresentazione precedente sono presenti tutti i vertici (con eventuali ripetizioni): quindi, ovviamente, il grafo è connesso (due vertici distinti qualsiasi li si ritrova presenti nella rappresentazione e, ovviamente, sono uniti da un cammino). Inoltre si vede che **coppie** di archi incidono su ogni vertice per cui il grado di ogni vertice è pari.

Seconda implicazione:

Ipotesi: è un grafo connesso con vertici tutti di grado pari;

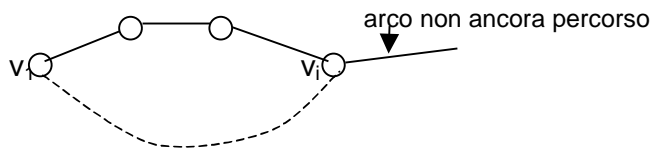
tesi: esiste un cammino ciclico Euleriano.

Fissiamo, a caso, un vertice v_1 : poiché non vi sono vertici isolati, su v_1 avremo almeno un arco (in realtà almeno 2, essendo il grado pari). $v_1 \text{ --- } v_2$

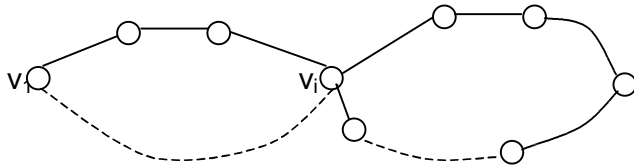
Costruiamo, a partire da tale primo arco, un cammino, procedendo con la seguente regola: ogni volta che si arriva su un vertice si esce dal vertice percorrendo (se possibile) un arco non ancora percorso. Tale procedimento, ad un certo punto, avrà termine quando si sarà giunti su un vertice v sul quale incidono archi tutti già percorsi. Ma tale vertice v sul quale siamo costretti ad interrompere il cammino è necessariamente il vertice v_1 : infatti, ogni volta che si arriva su un vertice $v_i \neq v_1$ e se ne esce, si utilizzano 2 archi incidenti su v_i (si devono cioè sottrarre tali 2 archi dal numero totale di archi incidenti su tale vertice) e quindi ogni volta che si arriva su v_i (utilizzando un arco) ne resta sempre almeno un altro (arco non ancora percorso) con il quale uscire dal vertice v_i , perché il grado di v_i è pari; quindi, quando il procedimento si interrompe (per l'impossibilità di uscire dal vertice percorrendo un arco non ancora percorso) il vertice sul quale si è giunti è v_1 (l'unico dal cui grado inizialmente si era *sottratto* 1, essendo il vertice di partenza).

Si è così costruito un cammino che parte dal vertice v_1 ed arriva sul vertice v_1 e che percorre alcuni archi del grafo, ognuno una ed una sola volta. Se gli archi di tale cammino sono tutti quelli del grafo, si è costruito il cammino Euleriano ciclico cercato.

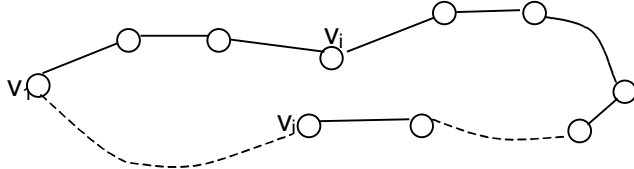
Supponiamo invece che vi sia qualche arco del grafo non ancora percorso. Ma il fatto che il grafo sia connesso (ipotesi) garantisce che vi è almeno un arco non percorso che incide su uno vertici del cammino costruito:



Ripartendo dal vertice v_i , con lo stesso procedimento fatto partendo da v_1 , si costruisce un cammino che parta da v_i ed arrivi su v_i , percorrendo archi una ed una sola volta; otterremo:



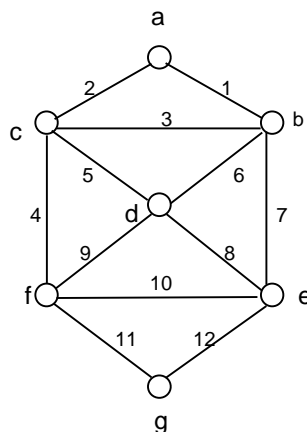
Poi si “spezza” il cammino nel vertice v_i per crearne uno unico:



Se tutti gli archi del grafo sono stati percorsi il teorema è dimostrato, altrimenti si procede ancora con il medesimo procedimento. Alla fine si otterrà il cammino Euleriano ciclico.

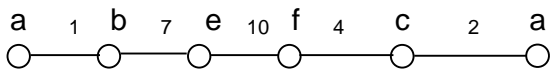
Lezione n°. 52 – 23 mar. 2001

Esempio: consideriamo un grafo con 7 vertici e 12 archi, connesso e tale che tutti i vertici hanno grado pari.

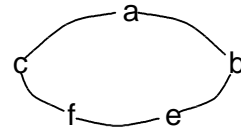


Costruiamo un cammino ciclico Euleriano (sarà sicuramente possibile per il teorema) seguendo l'algoritmo indicato nella dimostrazione del teorema di Eulero: si prende un vertice v a caso, un arco che incide su v e si comincia a costruire un cammino percorrendo

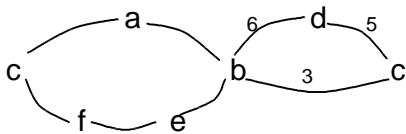
archi non ancora percorsi; il ragionamento garantisce che l'impossibilità di proseguire nel cammino si ha quando si è nuovamente sul vertice v di partenza. Ad esempio, scegliamo il vertice a :



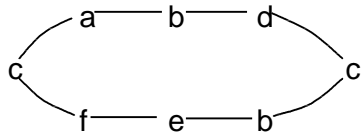
cioè la “collana”:



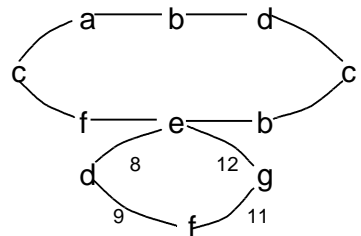
Consideriamo, fra gli archi non ancora percorsi (7 in tutto) almeno un arco che incide su uno dei vertici già toccati e ricominciamo il ragionamento. Per esempio, utilizziamo l'arco 6, incidente sul vertice b :



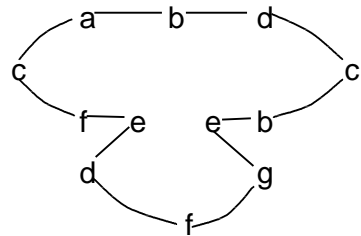
“Spezziamo” il cammino sul vertice b ed otteniamo:



Rimangono gli archi 8,9,11,12. Ne scegliamo uno incidente su uno dei vertici già toccati, ad esempio il 12 (incidente su e) e ricominciamo:

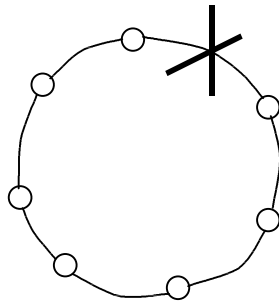


“Spezzando” il cammino sul vertice e , si ottiene il cammino ciclico Euleriano cercato:



Problema: se si cerca l'esistenza di un cammino Euleriano (ogni arco è percorso una ed una sola volta) ma non ciclico (cioè vertice di partenza diverso da quello di arrivo), quali sono le condizioni da imporre sul grafo?

Dato il cammino ciclico, per ottenerne uno non ciclico basta considerare il grafo ottenuto abolendo uno degli archi:



quindi le condizioni sono le stesse viste per i cammini ciclici con un'unica eccezione: ogni vertice deve avere grado pari tranne due che devono avere grado dispari (i vertici di partenza e di arrivo).

Il problema dei 4 colori (1850).

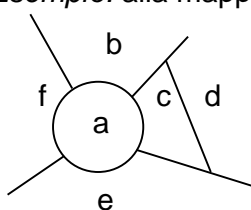
Presa una qualunque “mappa geografica” (intendendo per tale un piano suddiviso in zone confinanti), quanti colori sono necessari (al minimo) per colorare le regioni della mappa, con il criterio che 2 zone confinanti non abbiano mai lo stesso colore?

(Nota: si chiede il minimo numero di colori necessario per una qualunque mappa).

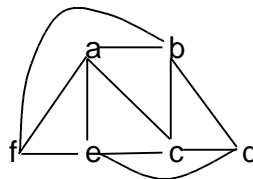
Nel 1976 si è dimostrato che 4 colori bastano sempre.

Formalizziamo il problema in termini di teoria dei grafi: una mappa geografica si trasforma in un grafo prendendo come vertici le regioni e disegnando un arco fra due vertici distinti quando le regioni corrispondenti sono confinanti.

Esempio: alla mappa seguente:



si associa il grafo:

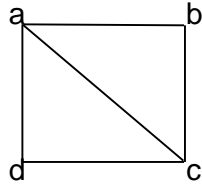


Se in un grafo chiamiamo “adiacenti” 2 vertici distinti che siano uniti da un arco, il problema della colorazione di una mappa si traduce nel problema dell’assegnazione ad ogni vertice del grafo corrispondente un colore in modo che vertici adiacenti abbiano colori diversi.

Formalmente: dato un grafo qualunque, una colorazione del grafo è un'applicazione che va dall'insieme V dei vertici all'insieme $\{1,2,3,\dots,n\}$ dei primi n numeri naturali (rappresentanti n colori distinti), tale che vertici adiacenti abbiano immagini ("colori") diversi.

Numero cromatico di un grafo è il minimo numero n di colori che servono per ottenere una colorazione del grafo.

Esempio: dato il grafo



si potrebbe ottenere una colorazione con 4 colori: $a \rightarrow 1$, $b \rightarrow 2$, $c \rightarrow 3$, $d \rightarrow 4$, ma ne bastano anche 3: $a \rightarrow 1$, $b \rightarrow 2$, $c \rightarrow 3$, $d \rightarrow 2$. due colori non bastano perché se $a \rightarrow 1$, siamo costretti ad associare b e d a 2 (perché sono adiacenti ad a) e siamo anche costretti ad utilizzare un 3° colore per c (che è adiacente ad a, b e d). Quindi il grafo ha numero cromatico uguale a 3.

Non esiste un criterio generale per il calcolo del numero cromatico di un grafo (ne dimostreremo per grafi con numero cromatico uguale a 2).

Il teorema dei 4 colori si traduce così: il grafo corrispondente ad una mappa geografica ha sempre numero cromatico ≤ 4 .

Nota: non tutti i grafi provengono da una mappa geografica.

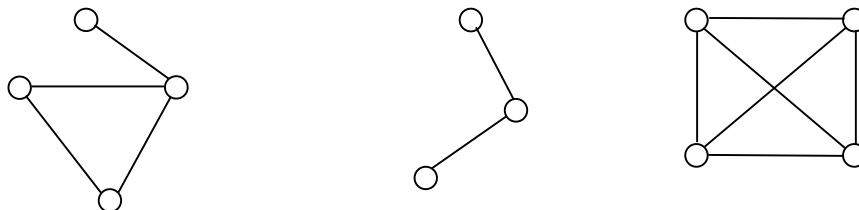
Componenti connesse di un grafo.

Un grafo è detto **connesso** se, comunque dati due vertici distinti, esiste almeno un cammino che li unisce. Si dimostra che, anche se il grafo non è connesso, lo si può suddividere in vari “sottografi” connessi. Si suppone, per semplicità, che il grafo non abbia vertici isolati (in quel caso un tale vertice si considera come “sottografo” connesso). Definiamo, nell'insieme V dei vertici del grafo, una relazione R , dicendo che un vertice v_1 è associato ad un vertice v_2 se esiste almeno un cammino che vada da v_1 a v_2 . Tale relazione R (da V in V) è una relazione di equivalenza, infatti gode delle proprietà:

1. RIFLESSIVA: preso un vertice v_1 , essendo esso non isolato, esisterà almeno un arco da v_1 ad un vertice v_2 , quindi esiste un cammino da v_1 a v_1 (si ottiene percorrendo l'arco da v_1 a v_2 e ripercorrendolo in senso inverso), quindi $v_1 R v_1$.
2. SIMMETRICA: non avendo gli archi un verso di percorrenza è ovvio che se vi è un cammino da un vertice v_1 ad un vertice v_2 allora ve ne è uno da v_2 a v_1 , cioè se $v_1 R v_2 \Rightarrow v_2 R v_1$.
3. TRANSITIVA: se $v_1 R v_2$ e $v_2 R v_3$ vi è un cammino da v_1 a v_2 ed un cammino da v_2 a v_3 per cui vi è un cammino da v_1 a v_3 , quindi $v_1 R v_3$.

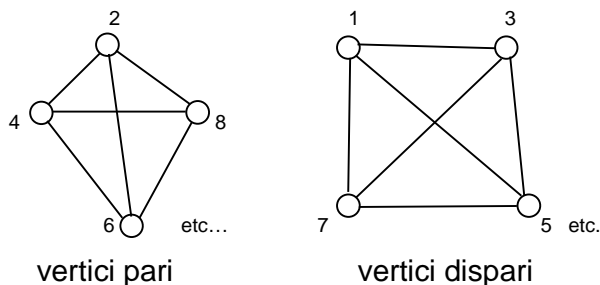
Se consideriamo una classe di equivalenza: $[v] = \{\text{vertici in relazione con } v\}$, due vertici di questa classe sono associati fra loro (per la proprietà transitiva di R) e quindi tra essi esiste un cammino e quindi tale classe, considerata come “sottografo” (cioè parte del grafo di partenza, ottenuta dai vertici della classe più gli archi ad essi relativi), è un grafo connesso detto **componente connessa del grafo di partenza**; quindi ripetendo il ragionamento, alla fine il grafo è suddiviso in componenti connesse.

Esempio 1: nel grafo seguente (che non è connesso) ci sono 3 componenti connesse:



Esempio 2: consideriamo come grafo la struttura che ha come vertici tutti gli interi fra 1 e 100 (estremi compresi) e dove due vertici distinti sono adiacenti (cioè uniti da un arco) se la loro somma è pari. Quali sono le componenti connesse del grafo?

Se due vertici sono entrambi pari o entrambi dispari sono uniti da un arco, se invece sono uno pari e l'altro dispari non lo sono. Il grafo è quindi diviso in due componenti connesse (globalmente invece il grafo non è connesso).



Si è definita *colorazione di un grafo* una applicazione

$$\{\text{insieme dei vertici}\} \rightarrow \{1, 2, \dots, n\} = \{\text{colori}\}$$

con la regola che due vertici distinti adiacenti (cioè uniti da un arco) non abbiano mai lo stesso colore associato. Si è inoltre definito *numero cromatico di un grafo* il numero n di colori necessari per una colorazione.

“Numero cromatico=1” equivale a dire che tutti i vertici sono isolati. Cosa significa “numero cromatico=2”? Per semplicità consideriamo grafo senza vertici isolati (d'altronde un vertice isolato può essere colorato a piacere). Come già visto, tale grafo si può suddividere in componenti connesse (sottografi, ognuno connesso) e, poiché tra vertici di due componenti connesse diverse non vi sono archi, il problema della colorazione del grafo si può affrontare separatamente per ogni componente connessa e quindi ridursi al caso in cui il grafo sia connesso.

Teorema: sia dato un grafo connesso: allora il grafo ha numero cromatico uguale a 2 se e solo se non esistono nel grafo cammini ciclici (cioè che partono da un vertice ed arrivano sullo stesso vertice) di lunghezza dispari (per *lunghezza di un cammino* si intende il numero di archi percorsi nel cammino stesso).

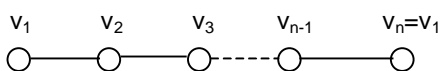
Dimostrazione.

Prima implicazione:

ipotesi: bastano 2 colori $\{1, 2\}$ per colorare il grafo;

tesi: il grafo non ha cammini ciclici di lunghezza dispari.

Supponiamo per assurdo che esista un cammino ciclico di lunghezza dispari:



il numero di archi nel cammino è dispari (per assurdo). Ma se coloriamo v_1 con il colore 1 siamo costretti a colorare v_2 con il colore 2 e v_3 nuovamente con il colore 1, v_4 con il colore 2 e così via alternando i colori 1 e 2: in generale il vertice v_{n-1} (essendo la lunghezza dispari) ha lo stesso colore di v_1 , quindi si ha una contraddizione dell'ipotesi.

Seconda implicazione:

ipotesi: non vi sono cammini ciclici di lunghezza dispari;

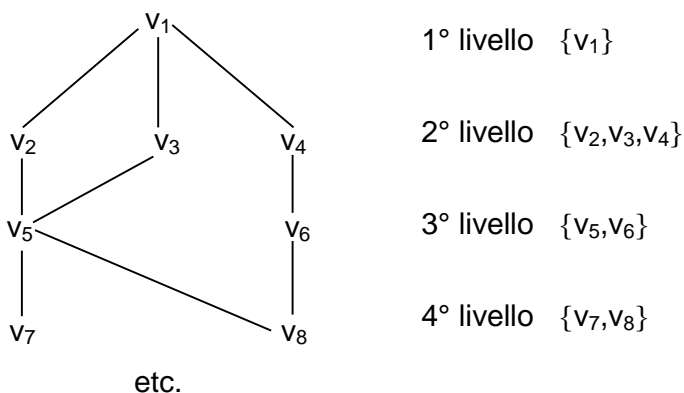
tesi: bastano 2 colori $\{1,2\}$ per colorare il grafo, cioè il numero cromatico del grafo è 2.

Lo scopo è quello di dare una regola per attribuire ad ogni vertice uno dei 2 colori. Suddividiamo l'insieme dei vertici del grafo in sottoinsiemi detti "livelli", fissiamo un vertice v_1 a piacere e, come livello 1 consideriamo l'insieme $\{v_1\}$; costruiamo il livello 2 considerando l'insieme di tutti i vertici adiacenti a v_1 :

v_1	Livello 1
Vertici adiacenti a v_1	Livello 2

Costruiamo il livello 3 considerando l'insieme di tutti i vertici adiacenti ad almeno un vertice del livello 2 e che siano diversi da v_1 ; nel livello 4 consideriamo tutti i vertici adiacenti ad almeno un vertice del livello 3 e che siano diversi dai vertici del livello 2 e così via.

Esempio:



Poiché la regola di inserimento in un livello evita la ripetizione dei vertici è certo che, essendo il numero dei vertici finito, vi sarà un termine al procedimento. Si osserva che, alla fine del procedimento, tutti i vertici del grafo sono inseriti in qualche livello; ciò è

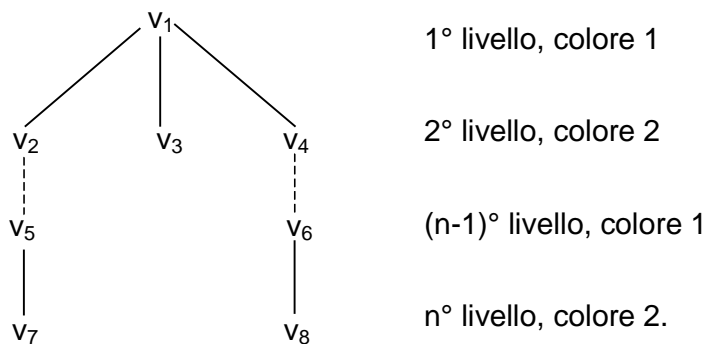
dovuto alla connessione del grafo (ipotesi del teorema): infatti, preso un vertice qualunque v , se esso è v_1 è nel 1° livello, se $v \neq v_1$, per la connessione del grafo, esiste sempre un cammino che unisce v a v_1 . Per la costruzione dei livelli v sarà in uno dei livelli costruiti.

Coloriamo il grafo con i due colori con la regola dell'alternanza sui livelli:

Livello 1	Colore 1
Livello 2	Colore 2
Livello 3	Colore 1
Livello 4	Colore 2
.....

Ci si deve assicurare che vertici distinti adiacenti abbiano colori diversi, ma due vertici adiacenti, per la costruzione dei livelli, sono presenti solo in livelli consecutivi (se il vertice v_i si trova nel livello n un vertice v_j adiacente a v_i si può trovare o al livello $n-1$ o al livello $n+1$) o nello stesso livello, ma quest'ultimo caso non si può presentare perché, se così fosse, si otterrebbe un cammino ciclico di lunghezza dispari (e ciò non può accadere per ipotesi).

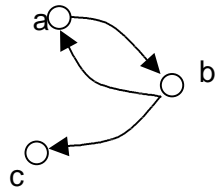
Schematicamente:



Grafi orientati.

In un grafo orientato vi sono i “vertici” e gli “archi” che li uniscono, ma ogni arco è “orientato” (cioè ha un verso di percorrenza) ed è rappresentato da una freccia.

Esempio:



I grafi in cui gli archi non hanno verso sono chiamati **grafi non orientati** o semplicemente grafi.

Il concetto di cammino in un grafo orientato è uguale a quello già definito per i grafi non orientati, ma il verso di percorrenza di ogni arco deve rispettare l'orientamento dell'arco stesso. Nell'esempio precedente si potrà costruire il cammino $a \rightarrow b \rightarrow c$ ma non si potrà costruire un cammino da c ad a.

Cammino Hamiltoniano.

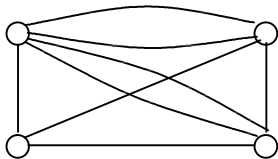
Dato un grafo (orientato o no) si dice **cammino Hamiltoniano** un cammino che tocchi tutti i vertici del grafo, ognuno una ed una sola volta.

È ancora un problema aperto la caratterizzazione dei grafi in cui esista un cammino Hamiltoniano. Si è però riusciti a dimostrare l'esistenza di un cammino Hamiltoniano in una particolare categoria di grafi, detti **grafi completi**.

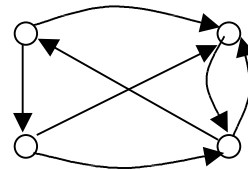
Un grafo (orientato o no) è detto **completo** se, comunque dati due vertici distinti, esiste sempre almeno un arco che li unisce.

Esempi di grafi completi:

grafo non orientato completo



grafo orientato completo



Teorema: in qualunque grafo completo (orientato o no) esiste sempre un cammino Hamiltoniano.

Dimostrazione: distinguiamo i due casi.

1. Grafo non orientato.

È ovvio; si parte da un vertice a caso v_1 , si prende un altro vertice $v_2 \neq v_1$ e si percorre un arco da v_1 a v_2 (che esiste per ipotesi); si prende quindi un vertice v_3 , diverso da v_1 e v_2 e si percorre un arco da v_2 a v_3 (che esiste per ipotesi) e così via, fino ad esaurire tutti i vertici del grafo, costruendo alla fine un cammino Hamiltoniano.

2. Grafo orientato.

Si prendono 2 vertici distinti v_1 e v_2 ; per ipotesi esiste almeno un arco che va da v_1 a v_2 o un arco che va da v_2 a v_1 . Supponiamo, ad esempio, che esista un arco che va da v_1 a v_2 : $v_1 \rightarrow v_2$. Cerchiamo di aggiungere nel cammino un 3° vertice v_3 diverso da v_1 e v_2 . Confrontiamo v_1 con v_3 : esiste (per ipotesi) almeno un arco che va da v_1 a v_3 o un arco che va da v_3 a v_1 ;

- nel primo caso (arco $v_1 \rightarrow v_3$) confrontiamo v_3 con v_2 : di nuovo esiste (per ipotesi) almeno un arco da v_3 a v_2 (nel qual caso consideriamo il cammino $v_1 \rightarrow v_3 \rightarrow v_2$) oppure un arco da v_2 a v_3 (nel qual caso consideriamo il cammino $v_1 \rightarrow v_2 \rightarrow v_3$).
- Nel secondo caso (arco $v_3 \rightarrow v_1$) consideriamo il cammino $v_3 \rightarrow v_1 \rightarrow v_2$.

In ogni caso si è riusciti a costruire un cammino che tocca tutti e 3 i vertici, ognuno una ed una sola volta.

In generale il procedimento consiste nell'aggiungere un nuovo vertice al cammino già costruito ed andare avanti fino ad esaurire tutti vertici.

Ma qual è l'algoritmo per passare da n vertici ad $n+1$ vertici?

Supponiamo di avere già costruito un cammino che tocca n vertici distinti:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_n$$

dato un ulteriore vertice $v_{n+1} \neq v_1, v_2, v_3, \dots, v_n$, lo scopo è la costruzione di un cammino che tocchi tutti vertici $v_1, v_2, v_3, \dots, v_n, v_{n+1}$, ognuno una ed una sola volta.

Si procede come segue:

confrontiamo v_{n+1} con v_1 :

- 1° caso: esiste un arco da v_{n+1} a v_1 e in questo caso il cammino cercato è:

$$v_{n+1} \rightarrow v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_n;$$

- 2° caso: esiste un arco da v_1 a v_{n+1} ; in questo caso si confronta v_{n+1} con v_2 e
 - 1° sottocaso (del 2° caso): se esiste un arco da v_{n+1} a v_2 il cammino cercato è:

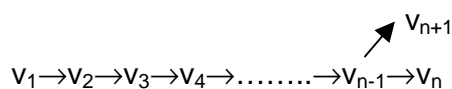
$$v_1 \rightarrow v_{n+1} \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_n;$$

- 2° sottocaso (del 2° caso): se esiste un arco da v_2 a v_{n+1} si crea la seguente situazione:

$$\begin{array}{c}
 \nearrow v_{n+1} \\
 v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_n
 \end{array}$$

In tal caso si confronta v_{n+1} con v_3 e si distinguono nuovamente 2 sottocasi (esiste un arco da v_{n+1} a v_3 oppure da v_3 a v_{n+1}) e si continua così il ragionamento.

Alla fine la situazione (nel caso non si sia riusciti ancora a costruire il cammino) è:



Si confrontano allora v_{n+1} con v_n ed anche qui vi sono due sottocasi:

- se c'è un arco da v_{n+1} a v_n e allora il cammino cercato è:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_{n+1} \rightarrow v_n;$$

- se invece esiste l'arco da v_n a v_{n+1} basta mettere in coda al cammino il vertice v_{n+1} , per ottenere il cammino Hamiltoniano:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \dots \rightarrow v_{n-1} \rightarrow v_n \rightarrow v_{n+1}.$$

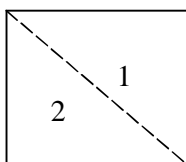
Lezione n°. 55 – 30 mar. 2001

Matrice di adiacenza di un grafo.

Problema: dato un grafo (orientato o no), e fissati 2 vertici, con quale algoritmo verificare se esiste un cammino dall'uno all'altro? E se esiste un tale cammino, qual è la sua lunghezza minima?

Si è definiti (nel caso di grafi non orientati) 2 vertici adiacenti se esiste un arco fra essi. Si può estendere la definizione anche al caso dei grafi orientati: un vertice a è adiacente ad un vertice b se esiste un arco da a a b (arco orientato: vertice di partenza a , vertice di arrivo b). Si può avere che il vertice a sia adiacente al vertice b ma non viceversa.

La relazione di adiacenza è una relazione dall'insieme V dei vertici in se stesso: ovviamente nel caso dei grafi non orientati la relazione gode della proprietà simmetrica. Si prevede la possibilità di cappi (si ricorda che i cappi sono archi che uniscono un vertice con se stesso) che permettono di stabilire se un vertice è in relazione con se stesso oppure no. Della relazione di adiacenza si può costruire la matrice (è una matrice quadrata con tante righe e colonne quanti sono i vertici del grafo): se il grafo è non orientato, tale matrice è simmetrica rispetto ad una diagonale:

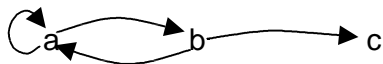


I due triangoli sono uno *specularmente* uguale all'altro.

La matrice della relazione di adiacenza è detta **matrice di adiacenza del grafo**.

Esempi:

1) il seguente grafo orientato



ha come matrice di adiacenza (una volta scelto l'ordine $\{a,b,c\}$):

	a	b	c
a	1	1	0
b	1	0	1
c	0	0	0

2) il seguente grafo non orientato



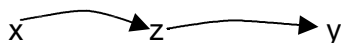
ha come matrice di adiacenza (una volta scelto l'ordine $\{a,b,c\}$) la matrice simmetrica:

	a	b	c
a	1	1	0
b	1	0	1
c	0	1	0

Nella matrice di adiacenza di un grafo i valori 1 corrispondono ai cammini di lunghezza 1 da un vertice ad un altro (cammino di lunghezza 1=singolo arco).

Ma cosa significa dire che da un vertice x ad un vertice y vi è un cammino di lunghezza 2?

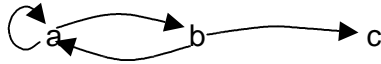
Significa che esistono un vertice z , un arco da x a z ed un arco da z a y :



in pratica si può definire una nuova relazione dall'insieme V dei vertici in se stesso, associando un vertice x ad un vertice y , quando esiste un cammino di lunghezza 2 da x a y . Tale relazione non è altro che la composizione della relazione di adiacenza con se stessa. La matrice di questa relazione composta è il prodotto booleano delle matrici delle due relazioni che si compongono; quindi, nel nostro caso, è il prodotto booleano della matrice di adiacenza per se stessa.

Conclusione: nella matrice ottenuta dal prodotto booleano della matrice di adiacenza per se stessa, le caselle contenenti un valore 1 corrispondono all'esistenza di cammini di lunghezza 2.

Esempio: in riferimento al grafo dell'esempio precedente:



La matrice di adiacenza del grafo è:

	a	b	c
a	1	1	0
b	1	0	1
c	0	0	0

Moltiplicando (con il prodotto booleano) la matrice per se stessa si ottiene:

1	1	0
1	0	1
0	0	0

X

1	1	0
1	0	1
0	0	0

=

1	1	1
1	1	0
0	0	0

I valori 1 nella matrice risultante corrispondono a cammini di lunghezza 2.

Il valore 1 nella 1^a casella della 1^a riga corrisponde al cammino di lunghezza 2 dal vertice a a se stesso: $a \rightarrow a \rightarrow a$ (il cappio è stato percorso due volte);

il valore 1 nella 2^a casella della prima riga corrisponde al cammino di lunghezza 2 da vertice a al vertice b: $a \rightarrow a \rightarrow b$ (si percorre il cappio e poi l'arco da a a b). etc.

Analogamente, si ottiene che il prodotto della precedente matrice moltiplicata ancora (con il prodotto booleano) per la matrice di adiacenza dà come risultato una matrice in cui i valori 1 corrispondono a cammini di lunghezza 3.

1	1	1
1	1	0
0	0	0

X

1	1	0
1	0	1
0	0	0

=

1	1	1
1	1	1
0	0	0

Problema: per decidere se vi è un cammino di lunghezza n dal vertice x al vertice y basta moltiplicare (con il prodotto booleano) n fattori uguali alla matrice di adiacenza e verificare se vi è il valore 1 all'incrocio fra la riga x e la colonna y della matrice risultante; ma per decidere se vi è un qualche cammino (di una certa lunghezza) da x a y , quante volte si deve moltiplicare la matrice per se stessa, prima di concludere che tale cammino non esiste. La risposta è: se m è il numero di vertici del grafo e se vi è un cammino da x a y , se ne può trovare sempre uno di lunghezza minore di m .

Dimostrazione: supponiamo di avere un cammino da x a y di lunghezza $\geq m$:

$$x = v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \dots \rightarrow v_k \rightarrow v_{k+1} = y$$

(la lunghezza k del cammino è di una unità inferiore al numero di vertici toccati, anche con ripetizione).

Ma se $k \geq m$ si ha $k+1 > m$, quindi il numero dei vertici toccati è superiore al numero totale m dei vertici del grafo quindi segue che si è toccato almeno un vertice 2 volte:

$$x = v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \dots \rightarrow v_i \rightarrow v_j \rightarrow \dots \rightarrow v_k \rightarrow v_{k+1} = y, \text{ con } v_i = v_j.$$

Si può allora abolire il *pezzo* di cammino fra v_i e v_j , ottenendo un cammino di lunghezza inferiore a quella iniziale k . Ripetendo il procedimento si ottiene alla fine un cammino di lunghezza $< m$, come voluto.

Conclusione: per decidere se vi è un cammino dal vertice x al vertice y , si prende la matrice di adiacenza, la si moltiplica per se stessa 2 fattori, 3 fattori, 4 fattori, ... $(m-1)$ fattori (dove m è il numero totale dei vertici). Se in una tale matrice si trova un valore 1 all'incrocio fra la riga x e la colonna y allora esiste un cammino da x a y , se ciò non avviene allora tale cammino non esiste.

Lezione n°. 56 – 2 apr. 2001

Operazioni in un insieme.

Prendiamo, per esempio, l'insieme \mathbb{Z} degli interi relativi. Sono definite in \mathbb{Z} le operazioni aritmetiche di somma e prodotto fra numeri interi.

La somma di due numeri interi $a, b \in \mathbb{Z}$ è una legge che associa ad ogni coppia di interi (a, b) , detti **addendi**, uno ed un solo numero intero (indicato con $a+b$) detto **risultato della somma**. Lo stesso discorso vale per il prodotto (sostituendo il simbolo $(a+b)$ con $(a \cdot b)$, il termine somma con prodotto ed il termine addendi con fattori).

In generale, dato un insieme A non vuoto, un'operazione in A è una legge che associa ad ogni coppia (a, b) di elementi di A (detti **operandi**) uno ed un solo elemento di A (indicato con $a*b$) detto **risultato**.

Esempi:

- nell'insieme dei numeri naturali $\mathbb{N} = \{1, 2, 3, \dots\}$ è definita l'operazione di elevamento a potenza: $a*b = a^b$ (il risultato è in \mathbb{N}).
- In \mathbb{Z} l'elevamento a potenza non è un'operazione perché, ad esempio:

$$2*(-3) = 2^{-3} = 1/8 \notin \mathbb{Z}.$$

- Se X è un insieme (non vuoto) fissato e si considera l'insieme A di tutte le applicazioni biunivoche $f: X \rightarrow X$, in tale insieme è definita l'operazione di composizione:

$\forall f, g \in A \quad f \circ g = g \circ f$ (il risultato è ancora in A, per le proprietà già viste nello studio delle applicazioni biunivoche)

Nel concetto generale di operazione non è previsto che il risultato dipenda o meno dall'ordine degli operandi. Se $\forall a, b \in A$ si ha sempre che $a * b = b * a$ si dice che l'operazione è **commutativa**.

Esempio: in \mathbb{Z} le operazioni di somma e prodotto sono commutative. In \mathbb{N} l'operazione di elevamento a potenza non lo è: per esempio $2^3 = 2^3 = 8$ è diverso da $3^2 = 3^2 = 9$.

Se l'insieme X ha almeno 3 elementi, allora l'operazione di composizione (nell'insieme A di tutte le applicazioni biunivoche da X a X) non è commutativa, infatti: se $X = \{a, b, c, \dots\}$ allora definiamo l'applicazione $f: X \rightarrow X$ come segue $f(a)=b$, $f(b)=a$, $f(c)=c$ e tutti gli altri eventuali elementi vengono associati con se stessi ($f(x)=x$). È ovvio che f sia biunivoca, quindi $f \in A$. Definiamo un'altra applicazione $g: X \rightarrow X$ come segue: $g(a)=a$, $g(b)=c$, $g(c)=b$ e tutti gli altri eventuali elementi vengono associati con se stessi ($g(x)=x$). Anche $g \in A$.

Calcoliamo $f \circ g$ e $g \circ f$.

$$f \circ g: \begin{cases} a \rightarrow b \\ b \rightarrow c \\ c \rightarrow a \\ \text{eventuali altri elementi associati a se stessi : } x \rightarrow x \end{cases}$$

$$g \circ f: \begin{cases} a \rightarrow c \\ b \rightarrow a \\ c \rightarrow b \\ \text{eventuali altri elementi associati a se stessi : } x \rightarrow x \end{cases}$$

In conclusione: $f \circ g \neq g \circ f$, quindi la composizione in A non è commutativa.

Se invece X ha 1 o 2 elementi allora, in A, l'operazione di composizione è commutativa:

se $X = \{a\}$ allora A contiene solo l'applicazione identica: $f(a)=a$ (ed $f \circ f = f \circ f$);

se $X = \{a, b\}$ allora A contiene $2! = 2$ applicazioni, che sono:

$$f: \begin{cases} a \rightarrow a \\ b \rightarrow b \end{cases} \quad (\text{applicazione identica}) \quad \text{e} \quad g: \begin{cases} a \rightarrow b \\ b \rightarrow a \end{cases} \quad \text{e si verifica facilmente che } f \circ g = g \circ f = g$$

Gruppo.

Esaminiamo in parallelo l'operazione di somma in \mathbb{Z} e l'operazione di composizione nell'insieme A (delle applicazioni biunivoche da X in X).

$\mathbb{Z}, +$	A, \circ
1. vale la proprietà associativa: $\forall a,b,c \in \mathbb{Z}, (a+b)+c=a+(b+c)$. (è noto). 2. esiste il numero 0 che è “neutro” rispetto alla somma: $\forall a \in \mathbb{Z}, a+0=0+a=a$. 3. comunque preso $a \in \mathbb{Z}$ esiste un intero $-a$ (detto opposto di a) tale che: $a+(-a)=(-a)+a=0$ (elemento neutro)	1. vale la proprietà associativa: $\forall f,g,h \in A, (f \circ g) \circ h = f \circ (g \circ h)$, infatti: $x \xrightarrow{h} y \xrightarrow{g} z \xrightarrow{f} t$ 2. esiste l'applicazione identica $\text{id} \in A$ che è “neutra” rispetto alla composizione: $\forall f \in A, f \circ \text{id} = \text{id} \circ f = f$, infatti: $f \circ \text{id} = x \xrightarrow{\text{id}} x \xrightarrow{f} y \quad \text{e} \quad \text{id} \circ f = x \xrightarrow{f} y \xrightarrow{\text{id}} y$ 3. comunque presa una $f \in A$ esiste f^{-1} (detta applicazione inversa di f) tale che: $f \circ f^{-1} = f^{-1} \circ f = \text{id}$ (elemento neutro).

In generale si definisce **gruppo** un insieme A (non vuoto) in cui è definita un'operazione $*$ tale che:

1. vale la proprietà **associativa**: $\forall a,b,c \in A, (a*b) * c = a * (b*c)$;
2. esiste un elemento **neutro** $e \in A$ tale che $\forall a \in A, a*e=e*a=a$ (in A può anche non valere la proprietà commutativa);
3. comunque preso un elemento $a \in A$, esiste $a' \in A$, detto **simmetrico** di a , tale che $a*a'=a'*a=e$ (elemento neutro).

Esempi:

1. \mathbb{Z} rispetto alla somma è un gruppo (elemento neutro=0, simmetrico di a =opposto di a);
2. $A=\{f:X \rightarrow X, f \text{ applicazione biunivoca}\}$ rispetto all'operazione di composizione è un gruppo (elemento neutro=id, simmetrico di una $f \in A$ =inversa di f).
3. \mathbb{Z} rispetto al prodotto non è un gruppo: vale la proprietà associativa, esiste l'elemento neutro (=1) ma non per tutti gli interi esiste il simmetrico in \mathbb{Z} (in genere è un razionale).
 $1*1=(-1)*(-1)=1$, quindi 1 e -1 sono simmetrici di se stessi, ma non esiste, ad esempio un $x \in \mathbb{Z}$ tale che $2*x=x*2=1$. In effetti solo 1 e -1 hanno simmetrico.
4. i razionali relativi \mathbb{Q} rispetto al prodotto non sono un gruppo: vale la proprietà associativa, esiste l'elemento neutro 1, ma lo 0 non ha simmetrico.

Ma $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ (insieme dei razionali relativi diversi da 0) rispetto al prodotto è un gruppo: vale la proprietà associativa, esiste l'elemento neutro 1 e per ogni $\frac{a}{b} \in \mathbb{Q}^*$ il simmetrico di $\frac{a}{b}$ è $\frac{b}{a}$.

Lezione n°. 57 – 4 apr. 2001

Monoide.

Si è definita operazione in un insieme A (non vuoto) una legge che associa ad ogni coppia (a,b) di elementi di A (operandi) uno ed un solo elemento $a*b$ di A (risultato). Se in A è definita un'operazione *. A è un gruppo se:

1. vale la proprietà **associativa**: $\forall a,b,c \in A, (a*b)*c = a*(b*c)$;
2. esiste un elemento **neutro** $e \in A$ tale che $\forall a \in A, a*e = e*a = a$;
3. comunque preso un elemento $a \in A$, esiste $a' \in A$, detto **simmetrico** di a, tale che $a*a' = a'*a = e$ (elemento neutro).

Vi è poi un'altra proprietà che può valere o no per un'operazione: la proprietà commutativa: $\forall a,b \in A, a*b = b*a$;

Se un insieme A, dotato di operazione *, soddisfa i punti 1 e 2 si dice che A è un **monoide**.

In un monoide non è detto che ogni elemento abbia simmetrico: per esempio, \mathbb{Z} rispetto al prodotto è un monoide (elemento neutro=1) e gli unici elementi che hanno simmetrico sono 1 e -1. In un monoide si definisce **simmetrizzabile** un elemento se esso ha un simmetrico nell'insieme A (in un gruppo tutti gli elementi sono simmetrizzabili).

Teorema:

in un monoide (e quindi anche in un gruppo) l'elemento neutro è unico; inoltre, per ogni elemento $a \in A$ simmetrizzabile, il simmetrico di a è unico.

Dimostrazione:

Unicità dell'elemento neutro: siano e_1, e_2 elementi neutri. Essendo e_1 neutro si ha che $e_1*e_2 = e_2$; essendo e_2 neutro si ha che $e_1*e_2 = e_1$ e, per l'unicità del risultato, si deduce che $e_1 = e_2$.

Unicità del simmetrico: se $a \in A$ ha due simmetrici $b, c \in A$ allora consideriamo il seguente elemento: $b*a*c = (b*a)*c = b*(a*c)$ (applicazione della proprietà associativa). Ma $b*a = e$ (elemento neutro) e anche $a*c = e$ (elemento neutro), essendo b e c simmetrici di a, quindi $e*c = b*e$; inoltre, $e*c = c$ e $b*e = b$, quindi $c = b$.

Teorema: se A è un monoide rispetto all'operazione $*$, l'insieme B di tutti gli elementi simmetrizzabili di A è un gruppo rispetto alla stessa operazione $*$.

Dimostrazione: B è un insieme non vuoto (almeno l'elemento neutro $e \in A$ ha simmetrico (se stesso: $e * e = e$). Prima verifichiamo che $*$ è un'operazione anche in B : comunque presi $a, b \in B$ (cioè a, b simmetrizzabili) è vero che $a * b \in B$? Cioè: $a * b$ è ancora simmetrizzabile? Chiamiamo c l'elemento $a * b$ e sia b' il simmetrico di b : allora

$$c * b' = (a * b) * b' = (\text{proprietà associativa}) = a * (b * b') = a * e = a;$$

sia a' il simmetrico di a : $c * (b' * a') = (c * b') * a' = a * a' = e$.

Analogamente si dimostra che anche $(b' * a') * c = e$ e che quindi $c = a * b$ è simmetrizzabile ed il suo simmetrico è $(b' * a')$.

Nota: il simmetrico di $a * b$ è $b' * a'$ (notare l'ordine inverso degli operandi).

Quindi $*$ è un'operazione anche nell'insieme B . Inoltre B è un gruppo rispetto all'operazione $*$, infatti:

1. vale la proprietà associativa (perché vale in A di cui è sottoinsieme);
2. l'elemento neutro $e \in A$ appartiene a B ed ovviamente è anche elemento neutro in B ;
3. se $a \in B$ esso ha simmetrico in B ? per costruzione di B l'elemento a ha certamente simmetrico $a' \in A$. Ma $a' \in B$ (perché ha simmetrico $a \in B$).

Esempio: \mathbb{Z} rispetto al prodotto è monoide ed i simmetrizzabili $\{1, -1\}$ formano un gruppo rispetto al prodotto stesso.

Tavola di un'operazione.

Se l'insieme A è finito ed è dotato di operazione $*$, si può descrivere l'operazione mediante una tavola (matrice nelle cui caselle si sistemano gli elementi di A): prima si fissa un ordine per gli elementi di A , $A = \{a_1, a_2, a_3, \dots, a_n\}$, si fanno corrispondere ordinatamente le righe e le colonne della tavola agli elementi a_1, a_2, \dots, a_n e nella casella all'incrocio fra la riga a_i e la colonna a_j si mette il risultato $a_i * a_j$.

Esempio: la tavola del prodotto per il gruppo $\{1, -1\}$ è:

	1	-1
1	1	-1
-1	-1	1

Esercizio: Come verificare la proprietà commutativa nella tavola? Come verificare se c'è un elemento neutro? Come verificare se un elemento ha simmetrico?

Lezione n°. 58 – 6 apr. 2001

Operazioni nell'insieme delle classi di congruenza.

Fissato un intero $n > 1$ nell'insieme \mathbb{Z} degli interi relativi, è definita la relazione di congruenza modulo m : $a \equiv b \pmod{m}$ se $(a-b) = k \cdot n$, con $k \in \mathbb{Z}$.

Tale relazione ripartisce \mathbb{Z} in n classi di equivalenza (dette classi di congruenza) ed il loro insieme è: $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$.

Definiamo in \mathbb{Z}_n due operazioni:

1. somma di classi definita da: $[a] * [b] = [a+b]$ ($a+b$ somma tra interi);
2. prodotto di classi, definito da: $[a] * [b] = [a \cdot b]$ ($a \cdot b$ prodotto tra interi).

Esempio: in \mathbb{Z}_8 sommiamo le classi $[7]$ e $[5]$: $[7] * [5] = [7+5] = [12] = [4]$ (si divide per 8 e si prende il resto, come visto in precedenza).

Moltiplichiamo le stesse classi: $[7] * [5] = [7 \cdot 5] = [35] = [3]$.

Per indicare somma e prodotto di classi si useranno, al posto del simbolo $*$, gli usuali simboli $+$ e \cdot : $[a] + [b] = [a+b]$ e $[a] \cdot [b] = [a \cdot b]$.

Ma, prima di continuare, bisogna verificare che il risultato delle operazioni di somma e prodotto fra classi sia unico, cioè che non cambi il risultato quando si cambia il rappresentante della classe, cioè:

1. se $[a] = [a']$, $[b] = [b']$ allora $[a+b] = [a'+b']$?
2. se $[a] = [a']$, $[b] = [b']$ allora $[a \cdot b] = [a' \cdot b']$?

Verifichiamo il punto 1: si ha che $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m} \Rightarrow a - a' = kn$ e $b - b' = hn$, con $k, h \in \mathbb{Z} \Rightarrow (a+b) - (a'+b') = (a-a') + (b-b') = (k+h)n \Rightarrow (a+b) \equiv (a'+b') \pmod{m} \Rightarrow [a+b] = [a'+b']$;

Verifichiamo il punto 2: si ha che $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m} \Rightarrow a - a' = kn$ e $b - b' = hn$, con $k, h \in \mathbb{Z} \Rightarrow (a \cdot b) - (a' \cdot b') = (a-a') \cdot b + a' \cdot (b-b') = (kb + a'h)n \Rightarrow (a \cdot b) \equiv (a' \cdot b') \pmod{m} \Rightarrow [a \cdot b] = [a' \cdot b']$.

(quanto sopra si ottiene moltiplicando $a - a' = kn$ per b , $b - b' = hn$ per a' e sommando membro a membro, etc.)

Esempio pratico: in $\mathbb{Z}_{12} = \{[0], [1], [2], \dots, [11]\}$, l'operazione di somma dà la cosiddetta "aritmetica dell'orologio": $[3] + [11] = [14] = [2]$.

Proprietà dell'operazione di somma fra classi.

La somma in \mathbb{Z}_n è commutativa: $[a]+[b]=[a+b]=[b+a]=[b]+[a]$ (dalla proprietà commutativa della somma fra interi). Inoltre \mathbb{Z}_n è un gruppo rispetto alla somma:

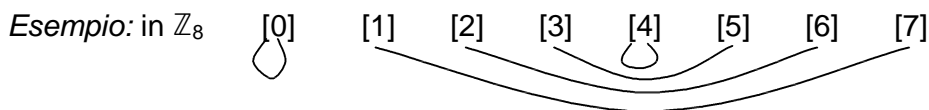
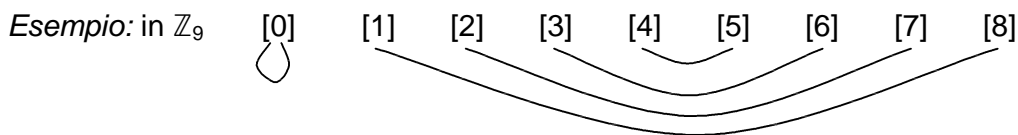
1. vale la proprietà associativa:

$$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]=[a+(b+c)]=[a]+[b+c]=[a]+([b]+[c]);$$

2. esiste l'elemento neutro che è $[0]$: $[a]+[0]=$ (commutatività) $=[0]+[a]=[a+0]=[a]$;

3. per ogni elemento $[a] \in \mathbb{Z}_n$ esiste il simmetrico: il simmetrico di $[0]$ è $[0]$ stesso ($[0]+[0]=[0]$). In generale, se prendiamo una $[a]$ compresa fra $[1]$ e $[n-1]$ allora il simmetrico di $[a]$ è $[n-a]$: $[a]+[n-a]=[a+(n-a)]=[n]=[0]$.

Quindi i simmetrici sono graficamente a "coppie simmetriche".



Allora \mathbb{Z}_n è un gruppo e vale anche la proprietà commutativa. Costruiamo la tavola dell'operazione di somma in \mathbb{Z}_3 :

	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Proprietà dell'operazione di prodotto fra classi.

Si verifica (come per la somma) che il prodotto fra classi è commutativo.

Vale inoltre la proprietà associativa (come per la somma) ed esiste l'elemento neutro che è $[1]$. Quindi \mathbb{Z}_n rispetto al prodotto fra classi è un monoide. Ma non è un gruppo: $[0]$ certamente non ha simmetrico (perché $[0]*[a]=[0]$ per ogni $[a]$) ma vi possono essere altre classi diverse da $[0]$ che non hanno simmetrico.

Esempio: in $\mathbb{Z}_4=\{[0],[1],[2],[3]\}$, $[2]$ non ha simmetrico:

$[2]*[0]=[0]$, $[2]*[1]=[2]$, $[2]*[2]=[4]=[0]$, $[2]*[3]=[6]=[2]$ cioè non si ottiene mai l'elemento neutro $[1]$.

Problema: quali sono le classi simmetrizzabili (fra le classi $[1],[2],\dots,[n-1]$), cioè le classi che hanno simmetrico?

Teorema: una classe $[a]$, con $a=1,2,3,\dots,(n-1)$ è simmetrizzabile in \mathbb{Z}_n rispetto al prodotto se e solo se $\text{mcd}(a,n)=1$ (cioè se a ed n sono coprimi).

Dimostrazione:

Prima implicazione – ipotesi: $[a]$ simmetrizzabile; tesi: $\text{mcd}(a,n)=1$.

Se $[a]$ è simmetrizzabile esiste il simmetrico $[b]$, cioè $[a]*[b]=[1] \Rightarrow [a*b]=[1] \Rightarrow a*b \equiv 1 \pmod{n}$, cioè $a*b-1=kn$, con $k \in \mathbb{Z}$, che possiamo scrivere come segue: $1=a*b-kn$ che è una combinazione lineare di (a,n) e, per un risultato già noto si deduce che $\text{mcd}(a,n)=1$.

Seconda implicazione – ipotesi: $\text{mcd}(a,n)=1$; tesi $[a]$ simmetrizzabile.

Per una proprietà del mcd , 1 è combinazione lineare di a,n : $1=a*a'+n*b'$, con $a',b' \in \mathbb{Z}$ (e che si possono calcolare con il metodo delle divisioni successive). Allora:

$a*a'-1=n*(-b')$ quindi $a*a' \equiv 1 \pmod{n}$, e quindi $[a*a']=[1] \rightarrow [a]*[a']=[1]$ e a' è il simmetrico di $[a]$, che si può quindi anche calcolare.

Esempio: in \mathbb{Z}_{12} $[7]$ avrà simmetrico perché $\text{mcd}(7,12)=1$, ma qual è? Si scrive 1 come combinazione lineare di 7 e 12 : $1=7*(-5)+12*3$ quindi il simmetrico di $[7]$ è $[-5]=(\text{ricordando quanto visto per le classi di congruenza})=[12-5]=[7]$. Verifichiamo l'esattezza di quanto trovato: $[7]*[7]=[49]=[1]$ (elemento neutro).

Lezione n°. 59 – 23 apr. 2001

Potenze di un elemento di un gruppo.

Se G è gruppo (con operazione $*$) e se a è un elemento di G , definiamo le potenze di a ad esponente intero positivo:

$$a^1=a;$$

$$a^2=a*a;$$

$$a^3=a*a*a;$$

:

$$a^m=a*a*\dots*a \text{ (dove } m \text{ è il numero degli operandi).}$$

Esempio: nel gruppo S_n (delle applicazioni biunivoche da $\{1,2,3,\dots,n\}$ in $\{1,2,3,\dots,n\}$ rispetto all'operazione di composizione), fissiamo, per esempio con $n=5$, l'elemento:

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

Allora

$$a^2 = a^0 a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \quad (\text{applichiamo due volte la funzione, quindi } 1 \rightarrow 2 \rightarrow 3, \text{ etc.});$$

$$a^3 = a^0 a^0 a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} \quad (\text{applichiamo tre volte la funzione});$$

etc.

Valgono per le potenze di un elemento di un gruppo le stesse proprietà delle potenze aritmetiche usuali: $a^{m+n} = a^m * a^n$ e $(a^m)^n = a^{mn}$,

(infatti, per esempio, $a^m * a^n = (\underbrace{a * a * \dots * a}_{m \text{ operandi}}) * (\underbrace{a * a * \dots * a}_{n \text{ operandi}}) = \underbrace{a * a * \dots * a}_{m+n \text{ operandi}} = a^{m+n}$)

Periodo di un elemento di un gruppo finito.

Sia G un gruppo finito e fissiamo un elemento $a \in G$. Dimostriamo che esiste qualche potenza di a che dà come risultato l'elemento neutro $e \in G$. Infatti: considerate le varie potenze di a , a^1, a^2, a^3, \dots , poiché esse sono in G (che è finito) non possono essere tutte elementi diversi di G , cioè esistono almeno due esponenti diversi k ed h (interi positivi) tali che $a^k = a^h$; supponiamo, per esempio, $h < k$; allora:

$$\underbrace{a * a * \dots * a}_{k \text{ operandi}} = \underbrace{a * a * \dots * a}_{h \text{ operandi}}$$

se a' è il simmetrico di a in G , componendo ambo i membri dell'eguaglianza con a' si ottiene: $\underbrace{a * a * \dots * a}_{k \text{ operandi}} * a' = \underbrace{a * a * \dots * a}_{h \text{ operandi}} * a'$

$$\begin{array}{ccc} \Downarrow & & \Downarrow \\ =e & & =e \end{array}$$

quindi l'eguaglianza diventa: $\underbrace{a * a * \dots * a}_{k-1 \text{ operandi}} = \underbrace{a * a * \dots * a}_{h-1 \text{ operandi}}$

Ripetendo tale procedimento h volte, alla fine si ottiene: $\underbrace{a * a * \dots * a}_{k-h \text{ operandi}} = e$

cioè $a^{k-h} = e$ con $k-h$ intero positivo. Cioè abbiamo trovato una potenza di a che dà l'elemento neutro. Fra tutte le potenze di a che danno l'elemento neutro (con esponente intero positivo) possiamo scegliere quella con esponente minimo (per l'assioma del buon ordinamento): questo esponente minimo è detto **periodo dell'elemento a** . Quindi, il periodo di un elemento a di un gruppo finito G è il minimo intero positivo che, dato come esponente alla base a , dà come risultato l'elemento neutro di G .

Esempio 1: in S_3 qual è il periodo di $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$?

L'elemento neutro è:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Calcoliamo le potenze di a :

$$a^1 = a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq e$$

$$a^2 = a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq e$$

$$a^3 = a \circ a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Quindi il periodo di $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ è 3

Esempio 2: l'insieme $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ delle classi di congruenza modulo 5, che è gruppo rispetto all'operazione di somma di classi. L'elemento neutro è $e = [0]$. Qual è il periodo di $a = [2]$?

$$[2]^1 = [2] \neq e;$$

$$[2]^2 = [2] + [2] = [4] \neq e;$$

$$[2]^3 = [2] + [2] + [2] = [6] = [1] \neq e;$$

$$[2]^4 = [2] + [2] + [2] + [2] = [8] = [3] \neq e;$$

$$[2]^5 = [2] + [2] + [2] + [2] + [2] = [10] = [0] = e.$$

Quindi il periodo di $[2] \in \mathbb{Z}_5$ è 5.

Osservazione: ovviamente l'elemento neutro in un gruppo G ha sempre periodo uguale ad 1.

Teorema di Lagrange.

Se G è un gruppo finito di ordine n , allora il periodo di un qualunque elemento di G è sempre divisore di n .

Dimostrazione: fissiamo un elemento $a \in G$ ed introduciamo una relazione R così definita:

$\forall x, y \in G \ x R y$ se esiste una potenza a^t di base a tale che $x = y * a^t$. Dimostreremo che R è una relazione di equivalenza.

[Premessa: chiamiamo k il periodo di a . Se consideriamo una qualunque potenza a^s di base a , dividendo s per k si ottiene: $s=kq+r$, con $0 \leq r < k$. Distinguiamo i due casi:

1° caso – $r > 0$: $a^s = a^{kq+r} = a^{kq} * a^r = (a^k)^q * a^r = (\text{poiché } a^k = e) = e^q * a^r = e * a^r = a^r$.

Quindi $s=r$ ed i valori possibili del resto sono $1, 2, 3, \dots, k-1$.

2° caso – $r=0$: allora $s=kq$ e $a^s = a^{kq} = (a^k)^q = e^q = e = a^k$.

Conclusione: una qualunque potenza a^s di base a coincide sempre con una delle seguenti potenze: $\{a^1, a^2, a^3, \dots, a^{k-1}, a^k\}$.

Inoltre tali potenze $\{a^1, a^2, a^3, \dots, a^{k-1}, a^k\}$ sono elementi distinti di G : infatti, se per assurdo 2 di esse coincidessero, ad esempio $a^v = a^z$ con $1 \leq v, z \leq k$, e se, per esempio $z < v$, ragionando come in precedenza, si otterrebbe $a^{v-z} = e$, ma $v-z < v \leq k$ e ciò è assurdo perché k è il periodo di a (che per definizione è il minimo intero positivo che, dato come esponente alla base a , dà come risultato l'elemento neutro e).

Concludendo, ogni potenza di a coincide con una delle seguenti potenze:

$\{a^1, a^2, a^3, \dots, a^{k-1}, a^k\}$ e tali potenze sono distinte e quindi in numero di k .]

Dimostriamo che R è relazione di equivalenza in G :

1. Proprietà riflessiva: $\forall x \in G \ x = x * e = x * a^k \Rightarrow xRx$;
2. Proprietà simmetrica: $\forall x, y \in G$ se xRy (cioè se esiste a^t tale che $x = y * a^t$) è vero che yRx ? Per la premessa sappiamo che $a^t = a^m$ con $m = 1, 2, 3, \dots, k-1, k$. Se $m=k$ si ha $a^t = a^k = e$, quindi $x=y$ e quindi yRx (per la proprietà riflessiva). Se invece $m < k$ allora $k-m$ è un intero positivo e si ha $y = y * e = y * a^k = y * a^{m+(k-m)} = y * a^m * a^{k-m} = (\text{essendo } a^m = a^t) = y * a^t * a^{k-m} = (y * a^t = x) = x * a^{k-m}$ cioè yRx .
3. Proprietà transitiva: se xRy (cioè $x = y * a^t$) e se yRz (cioè $y = z * a^v$) allora è vero che xRz ? $x = y * a^t = (z * a^v) * a^t = z * a^v * a^t = z * a^{v+t} \Rightarrow xRz$.

Lezione n°. 60 – 27 apr. 2001

Si è dimostrato che, se k è il periodo di un elemento a di un gruppo G , le potenze distinte di a sono esattamente in numero di k (tante quante il periodo) e sono $\{a^1, a^2, a^3, \dots, a^{k-1}, a^k\}$.

Consideriamo una classe di equivalenza rappresentata da un elemento $x \in G$:

$[x] = \{y \in G \text{ tale che } yRx, \text{ cioè } y = x * a^s, \text{ con } a^s \text{ potenza di base } a\} = \{x * a^1, x * a^2, \dots, x * a^{k-1}, x * a^k\}$.

Si noti che gli elementi $x * a^1, x * a^2, \dots, x * a^{k-1}, x * a^k$ sono distinti, perché se, per assurdo, 2 fra essi coincidessero (ad esempio $x * a^z = x * a^t$, se x' è il simmetrico di x , si avrebbe:

$$x' * x * a^z = x' * x * a^t = (\text{essendo } x' * x = e) = e * a^z = e * a^t \Rightarrow a^z = a^t$$

mentre si è dimostrato che $a^1, a^2, a^3, \dots, a^{k-1}, a^k$ sono distinti. Ciò porta alla conclusione che in ogni classe di equivalenza ci sono esattamente k elementi (dove k è il periodo di a),
Se c è il numero totale delle classi e se n è l'ordine di G allora si avrà:

$$n=|G|=k+k+k+\dots+k=c \cdot k$$

(c volte)

ossia che k è un divisore di n , che è la tesi del teorema di Lagrange che si voleva dimostrare.

Corollario: se G è un gruppo finito e se $n=|G|$ allora, comunque preso un elemento $a \in G$, si ha sempre $a^n=e$ (elemento neutro).

Dimostrazione: per il teorema di Lagrange, se k è il periodo di a , sappiamo che k è un divisore di n , ossia $n=k \cdot c$, con c intero, da cui si ottiene:

$$a^n = a^{kc} = (a^k)^c = (a^k = e \text{ essendo } k \text{ il periodo di } a) = e^c = e.$$

Dal risultato precedente segue il cosiddetto

Teorema di Eulero-Fermat.

Sia n un numero intero qualunque >1 e sia a un numero intero positivo coprimo con n (cioè $\text{mcd}(a,n)=1$). Se $\varphi(n)$ è la funzione di Eulero (cioè il numero di interi x compresi fra 1 ed n che sono coprimi con n) allora si ha: $a^{\varphi(n)} \equiv 1 \pmod{n}$ (ossia $(a^{\varphi(n)}-1)$ è multiplo di n).

Dimostrazione: sia \mathbb{Z}_n l'insieme di tutte le classi di congruenza modulo n , cioè:

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}.$$

Abbiamo introdotto in \mathbb{Z}_n l'operazione di prodotto fra classi $[x] \cdot [y] = [xy]$, rispetto alla quale \mathbb{Z}_n è un monoide (vale la proprietà associativa, esiste l'elemento neutro $e=[1]$, ma non tutti gli elementi di \mathbb{Z}_n sono simmetrizzabili: ad esempio $[0]$ non lo è e , fra tutte le altre classi $[1], [2], \dots, [n-1]$, lo sono solo quelle il cui rappresentante è coprimo con n).

Poiché gli elementi simmetrizzabili di un monoide formano un gruppo, tale gruppo, nel caso di \mathbb{Z}_n , è: $G = \{[x] \in \mathbb{Z}_n \text{ tale che } 1 \leq x \leq n-1 \text{ e } x \text{ è coprimo con } n\}$.

Il gruppo G ha ordine $\varphi(n)$. Per ipotesi abbiamo un intero $a > 0$ che è coprimo con n : allora, dividendo a per n si ottiene $a=nq+r$ con $0 \leq r \leq n-1$, ma $r \neq 0$ perché altrimenti a ed n non sarebbero coprimi, quindi $1 \leq r \leq n-1$.

Inoltre r è coprimo con n così come lo è a (se $d=\text{mcd}(r,n) \Rightarrow d$ è divisore di r e di $n \Rightarrow d$ è anche divisore di $a \Rightarrow d$ è divisore di a e di $n \Rightarrow d=1$ perché a ed n sono coprimi).

Quindi $[r] \in G$ e, per il corollario del teorema di Lagrange, si ha che $[r]^{\varphi(n)} = e = [1]$. Quindi

$$[1]=[r]^{\varphi(n)}=[r]*[r]*[r]*\dots*[r]=[r*r*r*\dots*r]=[r^{\varphi(n)}] \Rightarrow r^{\varphi(n)} \equiv 1 \pmod{n}$$

($\varphi(n)$ operandi)

Ma da $a = nq + r \Rightarrow (a-r) = nq$ e quindi che

$$a \equiv r \pmod{n} \Rightarrow [a] = [r] \Rightarrow [1] = [r]^{\varphi(n)} = [a]^{\varphi(n)} = [a^{\varphi(n)}] \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n} \text{ cioè la tesi.}$$

Esempio: sia $n=200=2^3 \cdot 5^2$ ed $a=37$ (a ed n sono coprimi). Il teorema di Eulero-Fermat dice che $37^{\varphi(200)} \equiv 1 \pmod{200}$. Ma $\varphi(200) = \varphi(2^3 \cdot 5^2) = \frac{200}{2 \cdot 5} \cdot (2-1)(5-1) = 20 \cdot 4 = 80$, quindi

$$37^{80} \equiv 1 \pmod{200}.$$

(Notare che 37^{80} è un numero molto grande e non si potrebbe ottenere facilmente l'informazione trovata con il teorema di Eulero-Fermat con il calcolo).

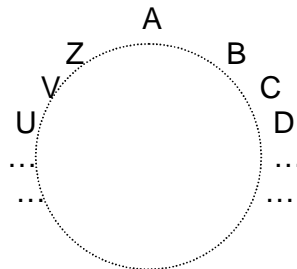
Lezione n°. 61 – 2 mag. 2001

Crittografia.

La crittografia è la scienza che studia il modo di trasformare un messaggio (con un procedimento detto **cifratura**) in un nuovo messaggio non comprensibile a terzi ed il modo di ritrasformarlo (**decifratura**) nel messaggio originario.

Esempio:

il “metodo di Cesare”: si dispongono le lettere dell'alfabeto circolarmente:



e si sostituisce ogni lettera del messaggio con quella ottenuta facendo “scivolare” la lettera di un numero k fissato di posizioni (scegliendo anche il verso, ad esempio in senso orario). Se $k=3$ si avranno le sostituzioni $A \rightarrow D$, $B \rightarrow E$, ..., $V \rightarrow B$, $Z \rightarrow C$.

Dall'esempio si vede che vi sono:

1. un algoritmo di cifratura (scivolamento delle lettere) che usa degli elementi ausiliari, **chiavi di cifratura** (nell'esempio vi è una sola chiave, che è k);
2. un algoritmo di decifratura (scivolamento in senso inverso delle lettere) che usa degli elementi ausiliari, **chiavi di decifratura** (nell'esempio la chiave di decifratura è sempre k).

Formalizziamo il processo:

per messaggio si è sempre inteso una successione di caratteri alfanumerici (lettere, numeri e segni di interpunzione) ma poiché il canale di trasmissione oggi è digitale, conviene trasformare preventivamente il messaggio in una successione di numeri (attraverso codici internazionali, ad esempio il codice ASCII). Quindi per messaggio si intende una successione di numeri.

Esempio:

il codice ASCII trasforma ogni carattere alfanumerico in un numero intero compreso tra 0 e 255 (esempi: A→64, B→65, spazio→32 etc.)

Allora un messaggio sarà una successione di numeri (ognuno compreso tra 0 e 255):

$\alpha_1\alpha_2\alpha_3\alpha_4\dots$ con $0 \leq \alpha_i \leq 255$.

In genere alcuni degli $\alpha_1\alpha_2\alpha_3\alpha_4\dots$ si “accorpano” insieme per ottenere numeri più grandi: si fissa un **numero base** N ed il messaggio da cifrare è prima trasformato in una successione di numeri interi β_i compresi tra 0 ed (N-1): $\beta_1\beta_2\beta_3\beta_4\dots$ con $0 \leq \beta_i \leq (N-1)$.

L’algoritmo di cifratura trasforma (servendosi delle chiavi di cifratura) la successione $\beta_1\beta_2\beta_3\beta_4\dots$ in una analoga $\gamma_1\gamma_2\gamma_3\gamma_4\dots$ (con γ_i sempre compreso tra 0 ed (N-1) che è il messaggio cifrato, mentre l’algoritmo di decifratura (servendosi delle chiavi di decifratura) applicato alla successione $\gamma_1\gamma_2\gamma_3\gamma_4\dots$ dà come risultato il messaggio originario $\beta_1\beta_2\beta_3\beta_4\dots$.

Considerando i singoli β_i si può dire che l’algoritmo di cifratura è un’applicazione $f:A \rightarrow A$, dove A è l’insieme di tutti i numeri interi β_i , con $0 \leq \beta_i \leq (N-1)$ e dove $f(\beta_i) = \gamma_i$, mentre l’algoritmo di decifratura è un’applicazione $g:A \rightarrow A$ tale che $g(\gamma_i) = \beta_i$.

Ossia $g \circ f =$ applicazione identica in A.

La situazione ottimale è che la conoscenza delle chiavi di cifratura non deve portare “facilmente” alla conoscenza delle chiavi di decifratura. Se il ricevente del messaggio conosce la chiave di decifratura egli è il solo responsabile della segretezza di tale chiave. Ma se è facile ricavare tale chiave da quella di cifratura, allora la segretezza è meno garantita.

Sistemi di crittografia a chiave pubblica.

Sono dei sistemi in cui la chiave di decifratura è segreta (e conservata solo dal ricevente dei messaggi) mentre la chiave di cifratura è pubblica (a patto che la chiave di decifratura sia “difficile” da ricavare a partire da quella di cifratura). Il più famoso di tali sistemi è il **sistema RSA** (dagli studiosi che lo misero a punto nel 1974: Rivest, Shamir ed Adleman).

Sistema RSA.

Si deve costruire l'algoritmo di cifratura $f:A \rightarrow A$ (con la chiave di cifratura) e l'algoritmo di decifratura $g:A \rightarrow A$ (con la chiave di decifratura). Poiché $A=\{x \in \mathbb{Z} / 0 \leq x \leq (N-1)\}$, si può "identificare" l'insieme A con l'insieme delle classi di congruenza modulo N :

$$\begin{array}{cccccccc} A = \{ & 0, & 1, & 2, & \dots & \dots & \dots & N-1 & \} \\ & \Downarrow & \Downarrow & \Downarrow & \dots & \dots & \dots & \Downarrow & \\ \mathbb{Z}_N = \{ & [0], & [1], & [2], & \dots & \dots & \dots & [N-1] & \} \end{array}$$

Con tale identificazione, l'algoritmo f (cifratura) diventa un'applicazione $f:\mathbb{Z}_N \rightarrow \mathbb{Z}_N$ e lo stesso vale per l'algoritmo g (decifratura): $g:\mathbb{Z}_N \rightarrow \mathbb{Z}_N$.

Descriviamo l'algoritmo f : si fissa N come prodotto di 2 numeri primi distinti (in genere molto grandi), quindi $N=pq$ (con p,q numeri primi distinti); si considera la funzione di Eulero $\varphi(N)$ e si fissa un intero positivo c tale che c sia coprimo $\varphi(N)$. Tale numero c sarà la chiave di cifratura. L'algoritmo f di cifratura è il seguente:

$f: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ così definito: $\forall [x] \in \mathbb{Z}_N \quad f([x]) = [x^c]$.

Descriviamo ora l'algoritmo di decifratura: consideriamo l'insieme $\mathbb{Z}_{\varphi(N)}$ di tutte le classi di congruenza modulo $\varphi(N)$; sappiamo che $\mathbb{Z}_{\varphi(N)}$ rispetto all'operazione di prodotto fra classi è un monoide (vale la proprietà associativa ed elemento neutro $= [1]$) e che gli elementi simmetrizzabili di $\mathbb{Z}_{\varphi(N)}$ sono le classi con rappresentante coprimo con $\varphi(N)$; quindi $[c] \in \mathbb{Z}_{\varphi(N)}$ è simmetrizzabile ed allora esiste una classe $[d] \in \mathbb{Z}_{\varphi(N)}$ tale che $[c][d] = [1]$ in $\mathbb{Z}_{\varphi(N)}$. Tale numero d sarà la chiave di decifratura e l'algoritmo di decifratura sarà:

$g: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ così definito: $\forall [x] \in \mathbb{Z}_N \quad g([x]) = [x^d]$.

Lezione n°. 62 – 4 mag. 2001

Algoritmo RSA.

Fissato un numero intero N prodotto di due numeri primi distinti, un messaggio è un numero intero compreso tra 0 ed $(N-1)$ o, equivalentemente, è una classe di congruenza modulo N compresa fra $[0], [1], \dots, [N-1]$; si sceglie un numero intero positivo c che sia coprimo con $\varphi(N)$ (funzione di Eulero di N) e, ricordando che $[c] \in \mathbb{Z}_{\varphi(N)}$ e che quindi esso sarà simmetrizzabile rispetto al prodotto fra classi, esisterà un'altra classe $[d] \in \mathbb{Z}_{\varphi(N)}$ tale

che $[c][d]=[1]$ (elemento neutro) in $\mathbb{Z}_{\varphi(N)}$; l'algoritmo di cifratura sarà $f([x])=[x^c]$ (chiave di cifratura=c); l'algoritmo di decifratura sarà $g([x])=[x^d]$ (chiave di decifratura=d).

Resta da dimostrare che effettivamente, decifrando il messaggio cifrato si ritorna al messaggio originale, e cioè che per ogni $[x] \in \mathbb{Z}_N$ $g(f([x]))=[x]$.

Per dimostrare ciò serve un teorema.

Teorema (di Rivet, Shamir, Adleman).

Sia N prodotto di due numeri primi distinti e sia t un numero intero tale che $t \equiv 1 \pmod{\varphi(N)}$.

Allora per ogni $[x] \in \mathbb{Z}_N$ si ha che $[x^t]=[x] \in \mathbb{Z}_N$.

Dimostrazione.

Sia $N=p \cdot q$ (con p,q numeri primi distinti). Per ipotesi $t \equiv 1 \pmod{\varphi(N)}$ quindi $t-1=k\varphi(N)$ (con k=numero intero) e cioè $t=1+k\varphi(N)$. Ma quanto vale $\varphi(N)$? Dalla formula nota si ricava:

$$\varphi(N) = \frac{N}{pq} (p-1)(q-1) = (p-1)(q-1)$$

La tesi è che $[x^t]=[x]$ per ogni $[x] \in \mathbb{Z}_N$. Distingueremo i vari casi possibili:

1° caso: sia x multiplo sia di p che di q, cioè x multiplo di N; in questo caso:

$$x=hN \text{ (con h intero) cioè } x \equiv 0 \pmod{N} \Rightarrow [x]=[0];$$

$$x^t = h^t N^t = (\text{essendo } x \text{ multiplo di } N) \Rightarrow x^t \equiv 0 \pmod{N} \Rightarrow [x^t]=[0], \text{ cioè la tesi.}$$

2° caso: sia x non multiplo nè di p, nè di q, cioè x non ha divisori comuni con N (tranne 1) e quindi $\text{mcd}(x,N)=1 \Rightarrow x$ ed N sono coprimi; per il teorema di Eulero-Fermat si ha:

$$x^{\varphi(N)} \equiv 1 \pmod{N}, \text{ cioè } [x^{\varphi(N)}]=[1].$$

Poiché $t=1+k\varphi(N)$ si ha:

$$[x^t]=[x^{1+k\varphi(N)}]=[x^1 x^{k\varphi(N)}] = (\text{regola sul prodotto fra classi}) = [x][x^{\varphi(N)}]^k = (\text{teorema di Eulero-Fermat}) = [x][1]^k = [x][1] = [x],$$

cioè la tesi.

3° caso: sia x multiplo di uno solo dei numeri p e q, per esempio sia x multiplo di p, e x non multiplo di q; consideriamo il numero intero x^t-x : se x è multiplo di p si ha $x=r \cdot p$ (con r intero) e $x^t=r^t p^t \Rightarrow x^t-x=p(r^t p^{t-1}-r)$ cioè x^t-x è multiplo di p. Poiché x non è multiplo di q, cioè q non è divisore di x, essendo q un numero primo esso ammette come divisori solamente 1 e q segue che 1 è l'unico divisore comune tra q ed x, cioè $\text{mcd}(x,q)=1 \Rightarrow q$ ed x sono coprimi. Allora, sempre per il teorema di Eulero-Fermat si ha $x^{\varphi(q)} \equiv 1 \pmod{q}$. Ma quanto vale $\varphi(q)$? Si ha che $\varphi(q)=q-1$ (tutti i numeri da 1 a q-1 sono coprimi con q, in quanto q è numero primo), cioè $x^{\varphi(q)}=x^{q-1} \equiv 1 \pmod{q}$.

Poiché $t=1+k\varphi(N)=1+k(p-1)(q-1)$ si ha che:

da $x^{q-1} \equiv 1 \pmod{q} \Rightarrow x^{q-1}-1=zq$ (con z =numero intero) e $[x^{q-1}]=[1]$ in \mathbb{Z}_q ;

$$[x^t]=[x^{1+k(p-1)(q-1)}]=[xx^{k(p-1)(q-1)}]=[x][x^{k(p-1)(q-1)}]^k=[x][x^{q-1}]^{k(p-1)} \stackrel{\text{(teor. di Eulero-Fermat)}}{=} [x][1]^{k(p-1)}=[x][1]=[x]$$

Si conclude che $[x^t]=[x]$ in \mathbb{Z}_q e cioè $x^t \equiv 1 \pmod{q}$ cioè x^t-x è multiplo di q . Quindi x^t-x è multiplo sia di p che di q e quindi è multiplo anche di $N=pq$ e cioè $x^t \equiv x \pmod{N}$ e cioè $[x^t]=[x]$ in \mathbb{Z}_N e cioè la tesi.

Tornando all'algoritmo RSA, i dati di partenza sono i seguenti:

N = prodotto di due numeri primi distinti;

c = numero intero coprimo con $\varphi(N)$;

$[d]$ = simmetrico di $[c]$ in $\mathbb{Z}_{\varphi(N)}$.

La tesi è che per ogni $[x] \in \mathbb{Z}_N$ $g(f([x]))=[x]$ dove f è l'algoritmo di cifratura e g quello di decifratura.

Ma $g(f([x]))=g([x^c])=[x^c]^d=[x^{cd}]$. Ora, posto $t=cd$, poiché $[d]$ è il simmetrico di $[c]$ in $\mathbb{Z}_{\varphi(N)}$, si ha che $[c][d]=[1]$ in $\mathbb{Z}_{\varphi(N)} \Rightarrow cd \equiv 1 \pmod{\varphi(N)}$ cioè $t \equiv 1 \pmod{\varphi(N)}$ e, per il teorema di RSA si ha: $[x^t]=[x]$ in \mathbb{Z}_N , ossia $[x^{cd}]=[x]$ e si è "tornati" (cifrando e decifrando) al messaggio originario, come volevasi dimostrare.

Esempio:

$N=11*13=143$ ($p=11$, $q=13$); messaggio=numero compreso tra 0 e 142 (oppure una classe di congruenza modulo 143 compresa tra $[0]$, $[1]$, ... $[142]$).

Si ha $\varphi(N)=(p-1)(q-1)=10*12=120$.

Fissiamo c (chiave di cifratura) coprimo con $\varphi(N)=120$, per esempio $c=13$. Il messaggio da cifrare sia, per esempio, il numero 3 (identificato con $[3]$): la cifratura sarà:

$f([3])=[3^{13}]=[1.594.323] \stackrel{\text{(dividendo per 143 e prendendo il resto)}}{=} [16]$, quindi 16 è il messaggio cifrato. Decifriamo adesso 16 e verifichiamo se si ottiene nuovamente il messaggio originario 3. Per decifrare serve la chiave di decifratura: $[d]$ è il simmetrico di $[c]=[13]$ in \mathbb{Z}_{120} . Per trovare $[d]$ il metodo è il seguente: si scrive $1=\text{mcd}(13,120)$ come combinazione lineare di $c=13$ e $\varphi(N)=120$ (con l'algoritmo delle divisioni successive) e si ottiene:

$$1=13*37+120*(-4).$$

Il coefficiente di $c=13$ il numero d cercato. Quindi, nel nostro caso, la chiave di decifratura è $d=37$.

Decifriamo il messaggio: $g([16])=[16]^{37}=[16^{37}]=\dots=[3]$ che è il messaggio originario.

NOTA: la facilità con la quale si è ricavata la chiave di decifratura d a partire dalla chiave di cifratura c consiste nella conoscenza dei numeri p e q singolarmente, per poter calcolare $\phi(N)=(p-1)(q-1)$. Se invece N viene reso pubblico con c ma si mantengono segreti i numeri primi p e q allora d è molto difficile da ricavare a partire da c (perché il calcolo di $\phi(N)$, non conoscendo la fattorizzazione di N in numeri primi, è difficile se N è grande).