- Matematica discreta. 01/10/13

- Connettivi logici (Booleani)

$\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

non è altro se non calcolare proposizioni (vere o false) 1 0

- Tavole di verità

A , B sono proposizioni

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
0	0	1	0	0	1	1
0	1		0	1	1	0
1	0	0	0	1	0	0
1	1		1	1	1	1

Il caso $A \rightarrow B$ è l'unico che merita di essere giustificato.

Definiamo però il predicato

Predicato = proposizione che dipende da alcuni parametri $P(x)$ $x > 3$

I connettivi si applicano a prop o predicati

Giustifichiamo $A \rightarrow B$ tramite i predicati

$x > 2 \rightarrow x^2 > 4$

La vogliamo vera per ogni x. Consideriamo i vari casi

A	B	$A \rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Prendiamo i vari casi

① $x = 3$, $3 > 2 \rightarrow 9 > 4$

(vero $\rightarrow$ vero) = vero 4ª riga

② $x = 1$ $1 > 2 \rightarrow 1 > 4$

(falso $\rightarrow$ falso) = vero 1ª riga

③ $x = -3$ $-3 > 2 \rightarrow 9 > 4$

(falso $\rightarrow$ vero) = vero 2ª riga

La 3ª riga non è scrivibile perché non è possibile scriverla. Infatti è l'unica falsa.

Per fare dimostrazioni si può: assumere "a" vera e verificare che anche "b" è vera

Prof A. Bernardeschi
Stanza 216 dip mat
Ricev: gio 15:00
ven 16:00
dan.unipi.it/a.bernardeschi
Argomenti importanti: da indicare in pdf.

• Quantificatori

$\forall x$ per ogni x $\quad \exists x$ esiste x — I quantificatori esplicano "quanti"

Predicato

$\exists x\ Q(x,y)$ vera o falsa a seconda di chi è y

$\exists x\,(x$ è figlio di $y)$ dove y = Maria — Questa è vera se Maria ha figli, altrimenti è falsa.

x ← variabile libera = nome oggetto

$\exists z \mid z$ è figlio di y — Rimaniamo le variabili legate (non libere)

Mentre $\quad \forall x \forall y\ P(x,y) \rightleftharpoons \forall y \forall x\ P(x,y)$

invece $\quad \forall x \exists y\ P(x,y) \not\rightleftharpoons \exists y \forall x\ P(x,y)$

• Negare un quantificatore

$\neg \forall x\ P(x) \rightleftharpoons \exists x \neg P(x)$

$\neg \exists x\ P(x) \rightleftharpoons \forall x \neg P(x)$

Esempio: D = numeri naturali $\mathbb{N}$

$\forall x \exists y \mid (x > y)$ → vera in $\mathbb{Z}$ / → falsa in $\mathbb{N}$ (0 non è maggiore di nulla)

$\exists y \forall x \mid (x > y)$ falso

$\forall y \exists x \mid (x > y)$ vera

$\forall x \forall y \mid (x > y)$ falso

$\exists x \exists y \mid (x > y)$ vera

• Predicato di appartenenza

Il simbolo $\in$ è detto predicato di appartenenza. Ne parliamo nell'ambito di "insiemi e classi".

Fissato un dominio e un predicato $P(x)$ diamo una classe: $\{x \mid P(x)\}$

Esempio: Dominio = persone, $P(x)$ = (x è un insegnante) allora

classe: $\{x \mid P(x)\}$ è la classe degli insegnanti

Se voglio esprimere "giorgio è insegnante" equivale a dire P(giorgio) oppure "giorgio $\in \{x \mid P(x)\}$"

dunque

$a \in \{x \mid P(x)\} \rightleftharpoons P(a)$

Consideriamo $\{x \mid P(x,y)\}$ classe che dipende da chi è y

Esempio: $\{x \mid x$ è amico di $y\}$ è la classe degli amici di y

Esempio 2: $\{x \mid x < y\}$ dove $y = 3$

Dominio $\mathbb{N}$ $\quad \{x \mid x < 3\} = \{0, 1, 2\}$

Cos'è una classe?

Negli insiemi/classi conta solo chi vi appartiene, non l'ordine ad esempio esempio: 23261 come n° di telefono non è $\{2,3,2,6,1\}$ perché esso è analogo a $\{1,2,3,6\}$

- Assioma di estensionalità:

  Insiemi X, Y quando sono uguali?

  Formalmente $\forall a\,(a \in X \rightleftharpoons a \in Y) \rightleftharpoons X = Y$

- Predicato di inclusione

  Viene rappresentato da $\subseteq$

  Esempio: Dominio = esseri viventi

  La classe insegnanti $\subseteq$ Classe mammiferi

  Formalmente se $X \subseteq Y \rightleftharpoons \forall a\,(a \in X \rightarrow a \in Y)$

Esempio: $\{a,b\} = \{c,d\}$ posso concludere che $a=c \wedge b=d$? NO 02/10/13

ad esempio $\{2,3\} = \{3,2\}$

Esempio 2: $\{a,b\}$ ha due elementi! Non è detto. Ad esempio se $a=b$ se $a=b=3$ abbiamo $\{a,b\} = \{3,3\} = \{3\}$

- Stringhe, coppie, terne...

  (a,b) nella coppia conta sia l'ordine che le ripetizioni (delle coppie ordinate)

esempio: $(a,b) = (c,d) \iff a=c \wedge b=d$

Triple $(a,b,c) = (a',b',c') \iff a=a' \wedge b=b' \wedge c=c'$

Posso anche vedere le triple come "coppie di coppie"

$(a,b,c) = ((a,b),c)$

- Prodotto cartesiano di insiemi

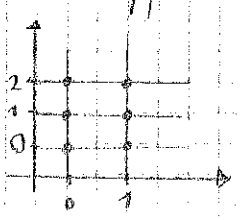
  A, B due insiemi

  $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$

esempio $A\{0,1,2\}$, $B=\{0,1\}$

$A \times B = \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}$

Li rappresentiamo nel piano



Cardinalità:

$|A|$ = cardinalità di A = n° di elementi di A. Nel nostro esempio:

N.B Posso esprimere le stringhe tramite insiemi ma non viceversa

Esempio: Esprimere la stringa 3 tramite insiemi. La teoria è quella di Kuratowsky

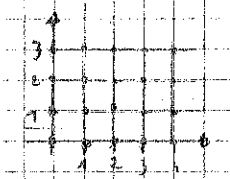
$(a,b) = \{\{a\},\{a,b\}\}$

$(3,4) = \{\{3\},\{3,4\}\}$

~~Una coppia coppia contenente due coppie~~

La coppia esattamente come $(a,b)^k = (c,d)^k$ con $a=c \wedge b=$

Esempio: Facendo $\mathbb{N} \times \mathbb{N}$ ottengo il primo cartesiano



In questo caso la cardinalità non è finita

$|A \times B| = |A| \cdot |B|$ se A, B sono finiti

Si può però parlare di diversi gradi di infinito (Cantor)

- Relazioni e funzioni

Esempio $(x < y)$ è una relazione tra numeri che dà risultato vero o falso

$(x+y)$ è una funzione che crea un nuovo valore

Def: In termini insiemistici, dati A, B insiemi, una relazione R tra A e B è un sottoinsieme di $A \times B$ dunque $R \subseteq A \times B$

Esempio 2: Il simbolo "$<$" in $\mathbb{N}$ è sottoinsieme di $\mathbb{N} \times \mathbb{N}$

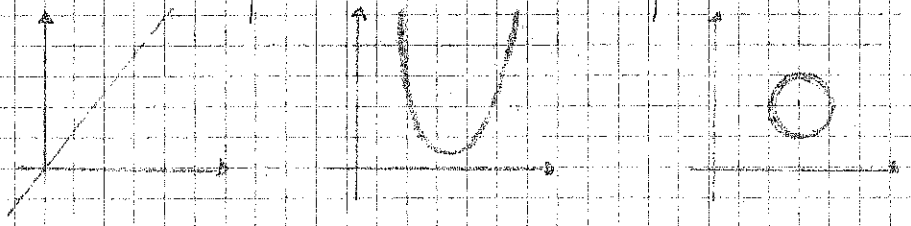
$(<) \subseteq \mathbb{N} \times \mathbb{N}$

Def: Una funzione $f: A \to B$ è una relazione $f \subseteq A \times B$ tale che:

se 1) $(a,b) \in f \wedge (a,b') \in f \Rightarrow b = b'$

2) per qualunque $a \in A$ deve esistere un $b \in B$ tale che $(a,b) \in f$

Dunque dico che $f(a) = b \iff (a,b) \in f$



- Quantificatori limitati

Esempio: Dominio = persone con $B = \{x \mid x \text{ è uno insegnante}\}$ dire $(\forall x \in B)(x$ è mancino$)$

Esempio 2: Sono equivalenti $(\forall x \in B)\, P(x) \iff (\forall x)[x \in B \to P(x)]$

esempio 3: $(\exists x \in B](P(x)) = \exists x (x \in B \wedge P(x)$

- Funzione

Def: $f \subseteq A \times B$ f è funzione da A a B se

1) $\forall a \in A,\ \forall b \in B,\ \forall b' \in B\ [(a,b) \in f \wedge (a,b') \in f \to b = b']$

2) $[\forall a \in A,\ \exists\, b \in B \mid (a,b) \in f$

Dunque $(a,b) \in f$ è equivalente ad $f(a) = b$ Quindi diciamo $f(a)$ l'unico b tale che $(a,b) \in f$

- Combinatoria

Quante funzioni ci sono da A a B?

esempio: $A=\{0,1,2\}$, $B=\{0,1\}$ esistono 8 funzioni, 2^3.

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
0	$\to 0$	$\to 0$	$\to 1$	$\to 0$	$\to 0$	$\to 1$	$\to 1$	$\to 0$
1	$\to 0$	$\to 0$	$\to 0$	$\to 1$	$\to 1$	$\to 0$	$\to 1$	$\to 1$
2	$\to 0$	$\to 1$	$\to 0$	$\to 0$	$\to 1$	$\to 1$	$\to 0$	$\to 1$

Prendiamone una.

$f_2 = \{(0,0), (1,0), (2,1)\}$

In generale se $|A| = n$, $|B| = k$ allora ci sono k^n funzioni possibili da A a B

Si giustifica che preso uno degli n elementi di A ho k possibilità per ognuno di essi dunque k ripetuto n volte $\underbrace{k \cdot k \cdot \ldots \cdot k}_{n \text{ volte}}$ dunque k^n

esempio 2: $A=\{0,1,2\}$, $B=\{0,1\}$ Quante relazioni ho?

Lo scopro trovando la cardinalità c di $A \times B$ ed eseguire 2^c

Dunque nel nostro esempio $c = 6 = |A \times B|$ dunque ho 2^6 possibili relazioni

Dimostrazione per ripetimento

- Insieme e sottoinsieme e parti

Dato un insieme A quanti sono i sottoinsiemi $X \subseteq A$? Ne ho $2^{|A|}$

$\mathcal{P}(A)$ = l'insieme dei sottoinsiemi

esempio: sia $A=\{0,1,2\}$ allora $\mathcal{P}(A) = \{X \mid X \subseteq A\}$ e infatti i sottoinsiemi possibili sono:

$\{\}$	$\{1\}$	$\{0,1\}$	$\{1,2\}$
$\{0\}$	$\{2\}$	$\{0,2\}$	$\{0,1,2\}$

sono tutti sottoinsiemi di A.

• Induzione

$\mathbb{N}$ = l'insieme dei numeri naturali $= \{0, 1, 2, \dots\}$ In $\mathbb{N}$ abbiamo una relazione del tipo $R \subseteq \mathbb{N} \times \mathbb{N}$, $(a,b) \in R \iff a \leq b$ che viene detta relazione d'ordine totale

def: $R \subseteq A \times A$ è una relazione di ordine totale su A se

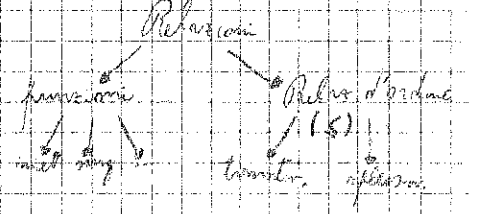
ordine ordine tot
1) $xRy \wedge yRz \to xRz$ (transitività)
2) xRx (riflessività)
3) $xRy \wedge yRx \to x = y$
4) $(\forall x \in A)(\forall y \in A)[xRy \vee yRx]$

N.B. la relaz. $\subseteq$ tra insiemi è un ordine non totale, sostituendo $\subseteq$ al posto di R, la 4) non si verifica

Esempio In $\mathbb{N}$ vi è un ordine totale

Esempio In quanti modi posso ordinare $\{0,1,2\}$ dunque quante relaz. d'ordine tot in $R \subseteq \{0,1,2\} \times \{0,1,2\}$ ci sono? Quella usuale ($\leq$ standard) è:
$R = \{(0,0), (0,1), (0,2), (1,1), (1,2), (2,2)\}$ cioè $0R1R2$

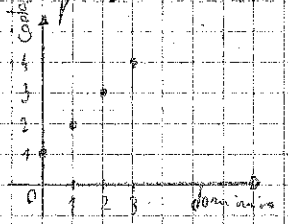
$0 R_1 1 R_2 2$ $\quad$ $1 R_3 2 R_3 0$
$0 R_1 2 R_1 1$ $\quad$ $2 R_4 0 R_4 1$
$1 R_2 0 R_2 2$ $\quad$ $2 R_4 1 R_4 0$



In $\mathbb{N}$ vi è una "funzione successore" $S: \mathbb{N} \to \mathbb{N}$ tale che

1) $S(x) = S(y) \to x = y$, è iniettiva
2) $\forall x \in \mathbb{N}$ $0 \neq S(x)$, non è suriettiva ma grazie (accetta per lo 0)
3) $(\forall x \in \mathbb{N})(x \neq 0 \to (\exists y \in \mathbb{N})(S\,y = x))$

Graficamente questa funzione è



Sia $f: A \to B$

A è dominio di f

B è codominio di f

L'immagine di f è l'insieme $\mathrm{Im}(f) \subseteq B$, $\mathrm{Im}(f) = \{f(a) \mid a \in A\} = \{x \in B \mid \exists a [x = f(a)]\} \subseteq$

Se $\mathrm{Im}(f) = B$ (cioè coincide col codom.) allora f è suriettiva

N.B. se $|A| = |B| = n \in \mathbb{N}$ allora f iniettiva $\iff f$ è surj

• Proposizioni

$\alpha \to \beta \equiv \neg\beta \to \neg\alpha$

α	β	$\alpha \to \beta$	$\neg\beta \to \neg\alpha$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Le due colonne si equivalgono

def iniettività $(\forall a \in A)(\forall a' \in A)$, $f(a) = f(a') \to a = a'$

suriettività $(\forall b \in B)(\exists a \in A) \mid f(a) = b$

In $\mathbb{N}$ abbiamo una relazione d'ordine $\leq$ e una funz $S: \mathbb{N} \to \mathbb{N}$ iniettiva collegate tra loro: $\forall x,\ x \leq S(x)$ cioè x è sempre $\leq$ del suo successore

$\neg \exists y [x < y \wedge y < S(x)]$ tra un numero ed il successivo non vi è niente

Da qui possiamo enunciare il principio d'induzione.

- Principio di induzione

Supponiamo che $P \subseteq \mathbb{N}$ tale che

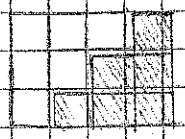
1) $P(0)$

2) $\forall x \in \mathbb{N} [P(x) \to P(S(x))]$ passo induttivo, $P(x)$ viene detta ipotesi induttiva

Allora $(\forall x \in \mathbb{N})\ P(x)$

9/10/13

Esempio $1+2+\dots+n = \frac{n \cdot (n+1)}{2}$ Visivamente

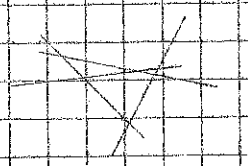


è un rettangolo di lati $n \cdot (n+1)$. Questa è l'area dei numeri da 1 a 3 presi due volte.

Altrimenti lo si verifica per induzione...

esempio 2: Prendo un cerchio e segno n punti sulla circonferenza. Traccio le corde dividendo il cerchio in regioni. Supponiamo che lo divida in 2^{n-1} parti. Verifico subito che con 6 punti ottengo 31 parti. Quale è la vera formula?

esempio 3: Date n rette nel piano e detto $a(n)$ il numero di punti in cui il piano viene suddiviso



n° rette	n° punti
1	2
2	4
3	7
4	11

Ogni retta aggiunge tante regioni quante punti sono i suoi punti di intersez con le rette precedenti $+1$

Supponiamo che aggiungendo una retta il numero di punti sia $a(n+1) = a(n) + (n+1)$

Notando che $a(4) = 2 + (2+3+4)$ anche $a(4) = 1+1+(2+3+4) = 1+(1+2+3+4)$

$= 1 + \frac{n(n+1)}{2}$

Adesso la verifico per induzione

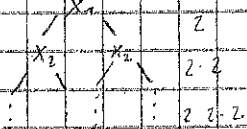
Lo dimostro per $n+1$.

$$Q(n+1) = Q(n) + n+1 = \left(\frac{n(n+1)}{2} + 1\right) + n + 1 = \frac{(n+1)(n+2)}{2} + 1$$

dunque è dimostrato

Esempio 4: Quanto un insieme X di n elementi quanti sono i suoi sottoinsiemi?

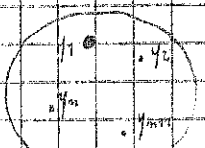
$|P(X)| = 2^n$?



Devo invece di dimostrarlo per induzione

$n=0$ $\quad P(\phi) = \{\phi\}$ $\quad |P(\phi)| = 2^0 = 1$

Lo voglio dimostrare per un insieme di $n+1$ elementi



} sottoinsiemi di questo insieme o contengo y_1 oppure no

Dunque: $P(y) = L_{cy_1} \cup L_{sy_1}$ dove $L_{cy_1} = \{A \subseteq y \mid y_1 \in A\}$

$L_{sy_1} = \{A \subseteq y \mid y_1 \notin A\}$

Quindi $|P(y)| = |L_{cy_1}| + |L_{sy_1}| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

Infatti $|L_{sy_1}| = 2^n$ perché l'insieme senza y_1 contiene n elementi ($n+1$ - 1 elemento) e dunque la sua cardinalità è 2^n

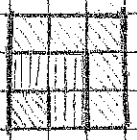
Inoltre la card di L_{cy_1} è uguale a quella di L_{sy_1} perché posso stabilire una funzione biettiva tra L_{cy_1} e L_{sy_1} della forma $L_{cy_1} \to L_{sy_1}$

Se la funzione è biettiva hanno l'insieme di partenza e arrivo hanno stesso n° di elementi

• Sommatorie e induzione 15/10/13

esempio: somma dei primi n numeri dispari positivi

$1+3+5+\dots+(2n-1) = \sum_{i=1}^{n} 2i-1$



congettura: $\sum_{i=1}^{n}(2i-1) = n^2$ ↑ P.M.I.

Adesso la verifichiamo per induzione $\forall n \geq 1$

$P(1)$: $\sum_{i=1}^{1}(2i-1) = 1 = n^2 = 1$ ✓ vera

presa per vera $P(n)$ verifico per $P(n+1)$

prendo per vera $\sum_{i=1}^{n}(2i-1) = n^2$ cerco di verificare $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$

$\sum_{i=1}^{n}(2i-1) + [2n+2-1] = n^2 + 2n + 1 \rightarrow 2n+1 = 2n+1$ vera ✓

Esempio 2: per quali $n \in \mathbb{N}$ $n^2 \leq 2^n$?

$2^{n+1} \geq (n+1)^2 \rightarrow 2\,2^n \geq (n+1)^2 \rightarrow 2n^2 \geq (n+1)^2 \rightarrow n^2 \geq 2n+1$

dimostro per induzione $(n+1)^2 \geq 2n+3 \rightarrow n^2+2n+1 \geq 2n+3 \rightarrow n^2 \geq 2$ ✓

è vera per tutti eccetto che per 3 da 5 a 30 ci sono 26 numeri

esempio 3: $\sum_{i=5}^{30}(4i+2) = \sum 4i + \sum_{i=5}^{30}(2) = 4\sum_{i=5}^{30} i + 2\cdot(26) = 4\left(\sum_{i=0}^{30} i - \sum_{i=0}^{4} i\right) + 52$

$= 4\left(\frac{30\cdot 31}{2} - 10\right) + 52 = 4\cdot 455 + 52 = 1872$

nota che $4i+2$ è una progr aritmetica. Per sommarle, fai come sopra

Esempio 4: progressione geometrica. Mi interessa la somma. Prendiamo 2^n. Di quanto fa $\sum_{i=0}^{7} 2^i = 1+2+4+8+16+32+64+128 = 2^8 - 1$

• Progressioni 16/10/13

aritmetica: se la differenza tra a_i e a_{i+1} sono costanti: $a_{i+1} - a_i = \text{cost}$.

Esempio: somma dei primi 100 termini di $2+3\cdot i$ cioè

$\sum_{i=0}^{99} 2+3\cdot i = \sum_{i=0}^{99} 2 + 3\sum_{i=0}^{99} i = 200 + 3\left(\frac{99\cdot 100}{2}\right) =$

geometrica: se il rapporto $\frac{a_{i+1}}{a_i}$ è costante

esempio: $1, 2, 4, \dots$ sommiamo i primi 100 termini

$\sum_{i=0}^{99} 2^i = 2^{n+1} - 1$ per induzione $\sum_{i=0}^{2n} 2^i = 2^{n+1} - 1$

a) per $n = 0$ è vera

$\sum_{i=0}^{n+1} \dots \sum_{i=0}^{n} \dots$

Esempio 2: progressioni con ragione x cerchiamo una formula che ci permetta

proviamo per induzione $\sum_{i=0}^{n} x^n = \frac{x^{n+1}-1}{x-1}$ (da fare per esercizio)

proviamo invece una dim per induzione: $\sum x^k = \frac{x^{n+1}-1}{x-1}$

$(x-1)\sum x_i = x^{n+1}-1 \rightarrow [(x+x^2+x^3+\dots+x^{n+1})-(1+x+\dots+x^n)] = x^{n+1}-1$

resta solo $x^{n+1}-1 = x^{n+1}-1$ ✓

- Induzione forte, ricorsione forte

ricorsione forte: per calcolare una certa grandezza mi riduco ad alcuni casi precedenti

esempio: successione di Fibonacci $f_0=1$, $f_1=1$, $f_{n+2} = f_{n+1}+f_n$

n	1	2	3	4	5	6
f_n	1	1	2	3	5	8

esercizio per n grande abbastanza $f_n \geq n^2 \rightarrow f_{n+2} \geq (n+2)^2$

inoltre $f_{n+2} = f_{n+1} + f_n \geq (n+1)^2 + n^2 \geq (n+2)^2$?

$n^2+2n+1+n^2 \geq n^2+4n+4 \rightarrow n^2+1 \geq 2n+3$

dimostro per induzione $(n+1)^2 \geq 2n+2+3 \rightarrow n^2+2n+1 \geq 2n+5 \rightarrow n^2 \geq 4$ vera per $n \geq 2$

Induzione forte: se riesco ad ottenere $P(n+2)$ sfruttando $P(n) \wedge P(n+1)$

riuscendo ad ottenere $P(n_0) \wedge P(n_0+1)$ allora $\forall n \geq n_0\ P(n)$

22/10/2018

- Formula esplicita per Fibonacci

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

dimostriamo per induzione che funziona, ma prima cerchiamo di capire come è stata costruita. Cerchiamo una successione f_n che verifichi la formula $f_{n+2} = f_{n+1} + f_n$ poiché Fibonacci cresce più velocemente di $n^2, n^3, \dots$ costruiamo una funzione che contenga α^n

cerco $\alpha^{n+2} = \alpha^{n+1} + \alpha^n$ dividendo per α^n $\alpha^2 = \alpha + 1$ risolvo allora l'eq di 2° grado $\Delta = 1+4 = (\sqrt{5})^2$ $\alpha_{1,2} = \frac{1 \pm \sqrt{5}}{2}$ ma così basi non funzionano

cerchiamo allora una eq della forma $c \cdot \alpha^n$, $c\alpha^{n+2} = c\alpha^{n+1} + c\alpha^n$

anche in questo caso, però non ci torna

N.B. esiste una analogia tra principio di induzione forte e principio del minimo

proviamo allora una combinazione lineare nella forma: $f_n = c\alpha^n + d\beta^n$

Ci chiediamo se $f_{n+2} = (c\alpha^{n+2} + d\beta^{n+2}) \overset{?}{=} (c\alpha^{n+1} + d\beta^{n+1}) + (c\alpha^n + d\beta^n)$

$$c\alpha^{n+2} + d\beta^{n+2} = c(\alpha^{n+1} + \alpha^n) + d(\beta^{n+1} + \beta^n)$$

ma noi sappiamo che $\alpha^{n+1} + \alpha^n = \alpha^{n+2}$ e lo stesso per β: dunque è verificata

La formula sarà del tipo: $f_n = c\left(\frac{1+\sqrt{5}}{2}\right)^n + d\left(\frac{1-\sqrt{5}}{2}\right)^n$

possiamo dire che $d = -c$ in quanto f_0 deve essere uguale a 0.

Se prendiamo f_1: $c\left(\frac{1+\sqrt{5}}{2}\right) - c\left(\frac{1-\sqrt{5}}{2}\right) = 1$ → [illegible]

$\frac{c+c\sqrt{5}}{2} - \frac{c+c\sqrt{5}}{2} = 1$ → $2c\sqrt{5} = 2$ → $c = \frac{1}{\sqrt{5}}$ dunque la formula sarà $f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

La dimostriamo ora per induzione $P(n) \wedge P(n+1) \to P(n+2)$

Ma questo è chiaro che abbiamo visto precedentemente! Dunque la formula è quella di Binet.

Esempio $a_1 = 4$, $a_2 = 22$, $a_3 = 82$ $\quad a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$

per trovare a_n procedo come prima cioè $a_n = x^n$ deve essere che

$x^4 = 6x^3 - 11x^2 + 6x$ → $x^3 = 6x^2 - 11x + 6$ che ha soluzioni

$x = 1, 2, 3$ quindi allora $a_n = c \cdot 1^n + d2^n + e3^n$

- Principio del minimo

Ogni insieme non vuoto di numeri naturali ha un minimo

esempio: Siano $a, b \in \mathbb{N}$, $b > 0$ allora esiste $q \in \mathbb{N}$, $r \in \mathbb{N}$ con $a = qb + r$ con $0 \leq r < b$.

Sia n minimo tale che $b(n+1) > a$ allora avremo che $bn \leq a < b(n+1)$ prendo $q = n$ e $r = a - bn < b$

Esempio 2: un numero è primo se è divisibile per 1 e per se stesso. Se $a \in \mathbb{N}$ è primo

$a = bn \to b = 1 \vee n = 1$

$x \mid y$ (x divide y) $\leftrightarrow \exists n\,[y = nx]$

ogni $n \neq 0$ è divisibile per un primo. La dimostriamo tramite il princip.

del minimo. Ho 2 casi: o è primo e allora ho finito, o non lo è. Dunque $n = ab$ con $a, b \neq 1$ ma ricordando $a < n$, $b < n$. Adesso possiamo vedere se a è divisibile per un primo o se b è divisibile per un primo. Abbiamo nuovamente 2 casi per "a" e 2 casi per "b". Prima o poi avremo un numero divisibile per un primo poiché se a è divisibile per un primo lo è anche n, altrimenti è finito.

- Coefficienti binomiali, cardinalità

23/10/13

$\exists$ biiezione $f: X \to Y \iff |X| = |Y|$

$\forall X$ $P(X) = \{Y \mid Y \subseteq X\}$ $P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{3,1\}, \{1,2,3\}\}$

Consideriamo le stringhe binarie di lunghezza 3 esse sono

1	2	3	
0	0	0	$\to \emptyset$
0	0	1	$\to \{3\}$
0	1	0	$\to \{2\}$
1	0	0	$\to \{1\}$
0	1	1	$\to \{2,3\}$
1	1	0	$\to \{1,2\}$
1	0	1	$\to \{1,3\}$
1	1	1	$\to \{1,2,3\}$

Sono 8

Dove 0 sta per dire "non c'è" e 1 "c'è" ad esempio nella prima riga abbiamo 000 cioè "non c'è né 1, né 2, né 3" e questo corrisponde all'insieme vuoto.

Consideriamo adesso $\mathbb{N}_4 = \{1,2,3,4\}$ quanti sono gli ins che contengono 2 elementi?

$\binom{4}{2} = |P_2(\mathbb{N}_4)|$ $P_2(\mathbb{N}_4) = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

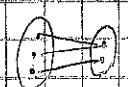
- Funzioni iniettive

29/10/13

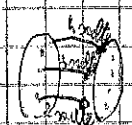
$D_{n,k}$ = numero delle funzioni iniettive da $\mathbb{N}_n$ a $\mathbb{N}_k$

$= |I_{n,j}(\mathbb{N}_n, \mathbb{N}_k)|$

Esempio: $D_{3,2} = 0$ non esistono funz iniettive da ins di 3 elementi a ins di 2 elementi. se $k < n \Rightarrow D_{n,k} = 0$ Assumo $k \geq n$

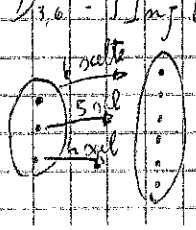


esempio 2: $D_{3,4} = |I_{n,j}(\mathbb{N}_3, \mathbb{N}_4)|$



Per il primo ho 4 scelte, per il secondo ho 3 scelte, per il terzo ho 2 scelte. Dunque $4 \cdot 3 \cdot 2$

Esempio 3: $D_{3,6} = |I_{n,j}(\mathbb{N}_3, \mathbb{N}_6)| = 6 \cdot 5 \cdot 4 = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1} = \frac{6!}{3!}$



In generale avrò che $|I_{n,j}(\mathbb{N}_a, \mathbb{N}_b)| = \underbrace{b \cdot (b-1) \cdots}_{a} = \prod_{i=0}^{a-1} (b-i) = b \cdot (b-1) \cdots (b-a+1) = \frac{b!}{(b-a)!}$

In generale da un'insieme di k ad uno di n elementi ho: $\frac{n!}{(n-k)!}$ funzioni iniettive

se invece voglio TUTTE le funzioni da ~~l'insieme~~ da insieme di k ad n elementi

ne ho $\underbrace{n \cdot n \cdots n}_{k \text{ volte}} = n^k$

Esempio: stringhe di lunghezza 5 di elementi in $\{0, \ldots, 9\}$ senza ripetizioni

0	8	1	6	3

dunque quelle qui sono $10 \cdot 9 \cdot \ldots \cdot 6 = \frac{10!}{(10-5)!}$

proprio come per le funz. iniettive.

se invece avessi avuto le ripetizioni avrei avuto $10 \cdot 10 \cdots 10 = 10^5$

modi possibili

Vorrei adesso contare gli insiemi di k elementi presi da un insieme di n elementi

sono $\binom{n}{k}$

esempio: Insiemi di 5 elementi presi da un insieme di 10 elementi $\binom{10}{5} = \frac{10!}{(10-5)! \cdot 5!}$

Nel complesso

$$\mathcal{P}(X) = \{ y \mid y \subseteq X \}, \quad \mathcal{P}_k(X) = \{ y \mid y \subseteq X \wedge |y| = k \}$$

esempio: $\mathcal{P}(\{1,2,3\}) = \{ \emptyset, \ldots, \{1,2,3\} \}$ inoltre $|\mathcal{P}\{1,2,3\}| = 2^3$

esempio 2: $\mathcal{P}_2(\{1,2,3\}) = \{ \{1,2\}, \{1,3\}, \{2,3\} \}$ inoltre $|\mathcal{P}_2\{1,2,3\}| = \binom{3}{2} = 3$

* Esercizi con calcolo combinatorio

1/

Targa italiana, 2 lettere 3 cifre 2 lettere abbiamo $26^2 \cdot 10^3 \cdot 26^2$ possibili targhe. Quante targhe invece hanno almeno una "7" ed una "a"

Io calcolo come

tutte le targhe $-$ (targhe senza a) $\cup$ (targhe senza 7))

dove la parte in parentesi è uguale a

$25^4 \cdot 10^3 + 26^4 \cdot 9^3 - \underbrace{25^4 \cdot 9^3}_{\text{targhe senza "a" ne "7"}}$

Dunque nel complesso:

$26^4 \cdot 10^3 - (25^4 \cdot 10^3 + 26^4 \cdot 9^3 - 25^4 \cdot 9^3) =$

2/

52 carte 4 semi

In quanti modi posso ricevere le carte? $\binom{52}{5} = \frac{52!}{47!\,5!}$

Quante doppie coppie esistono? Scelgo 2 valori che formeranno le coppie. Quanti sono? $\binom{13}{2}$. Scelgo poi il valore della carta restante che posso fare in 11 modi.

Scelgo il seme per il valore più basso $\frac{4\cdot 3}{2} = \binom{4}{2}$. Scelgo il seme per l'altra coppia che è di nuovo $\binom{4}{2}$. Infine scelgo il seme dell'ultima carta cioè moltiplico per 4.

Dunque $\binom{13}{2}\binom{4}{2}\binom{4}{2}\,11\cdot 4$

3/

(6,3) In quanti modi posso arrivare a (6,3)?

Avrò una stringa di lunghezza 9.

3 movimenti verso l'alto e 6 verso destra

Dunque $\binom{9}{6}$

Esercizi 30/10/13

1/

urna con 2 palline gialle, 2 rosse, 2 blu, 1 verde. TOT = 7

a) probabilità stesso colore?

b) quante possibili estrazioni di 2 palline?

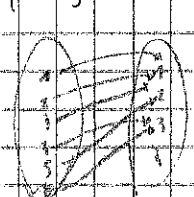
a) $\frac{2}{7}\cdot\frac{1}{6} + \frac{2}{7}\cdot\frac{1}{6} + \frac{2}{7}\cdot\frac{1}{6} = \frac{3\cdot 2}{7}\cdot\frac{1}{6} = \frac{6}{42} = \frac{1}{7}$

b) $\binom{7}{2} = \frac{7!}{5!\,2!} = \frac{7\cdot 6}{2!} = 7\cdot 3 = 21$

2/

Consideriamo le funzioni $f : [2m] \to [4]$ con $[n] = \{1, 2, \dots, n\}$

Ho 4^{2m} funzioni possibili. Cioè 4^{2m}. Voglio considerare quelle in cui $\{1,4\} \subset \mathrm{Im}(f)$ ad esempio:



In questi casi conviene calcolare tutte quelle che non vanno bene cioè: (quelle senza 1) $\cup$ (quelle senza 4) $= S_1 \cup S_4$

dove $|S_1| = 3^{2m}$ e $|S_4| = 3^{2m}$ dunque $|S_1 \cup S_4| = 3^{2m} + 3^{2m} - 2^{2m}$

quindi quelle che vanno bene sono $4^{2m} - 2\cdot 3^{2m} + 2^{2m}$

3/
Quante sono le stringhe binarie con 3 uni e 4 zeri?
$\binom{7}{3} \cdot 1$ è in effetti è uguale a $\binom{7}{4}$

4/
Quante sono le soluzioni $\{(x,y,z) \in \mathbb{N}^3 \mid x+y+z = 11\}$
conviene dare corrispondenza tra le triple e le stringhe binarie ad esempio
$(2,5,4) \longrightarrow (11)0(11111)0(1111)$ sono stringhe lunghe 13, con 11 uni.
2 la virgola 5 4
Dunque $\binom{13}{11} = \frac{13!}{2!\,11!} = \frac{13\cdot 12}{2!} = 13\cdot 6 = 78$

5/
Anagrammi di ASINO?
Avendo ripetizioni 5 caselle la soluzione è 5!
5 scelte, 3 scelte, 1 scelta, 1 scelta

Anagrammi di Mamma?
$\binom{5}{2} = \frac{5!}{3!\,2!} = \frac{5\cdot 4}{2!} = 10$ (0 1 0 0 1)

Anagrammi di ATTILIO? Si può fare in 2 modi
1) scelgo la posizione delle 2a $\binom{7}{2}$
2) scelgo la pos delle 3t $\binom{5}{3}$ $\binom{7}{2}\cdot\binom{5}{3}\cdot\binom{4}{2} = \frac{7!}{5!\,2!}\cdot\frac{5!}{4!\,1!}\cdot\frac{4!}{2!\,2!} = \frac{7\cdot 6}{2}\cdot\frac{5}{1}\cdot\frac{4\cdot 3}{2} = 7\cdot 6\cdot 5\cdot 3$
3) " " 2 l $\binom{4}{2}$ = 7·6·5·4·3·2
4) " dell'unica I = 1

$\frac{7!}{5!\,2!}\cdot\frac{5!}{4!\,1!}\cdot\frac{4!}{2!\,2!} = \frac{7!}{2!\,2!\,2!}$ (2·2·2 = n° delle a, 3·2 = n° delle t, 2 = n° delle l)

regola generale

6/
Avendo una scacchiera 3×3 con colorazioni binarie di neve
1) In quanti modi posso colorarla? 2^3
2) Quante affinché ogni riga sia diversa? $2^3\cdot(2^3-1)\cdot(2^3-2)$
3) Tutte una riga bianca? $3\cdot(2^3-1)\cdot(2^3-1)$
4) Una bianca = TUTTE − nessuna bianca $= 2^9 - (2^3-1)(2^3-1)(2^3-1)$
5) almeno una riga monocolore $= 2^9 - (2^3-2)(2^3-2)(2^3-2)$

- Binomio di Newton
la somma dei valori della n-esima riga è 2^n infatti:
$2^5 = (1+1)^5 = \sum_{i=0}^{5}\binom{5}{i}1^i\cdot 1^{5-i}$

3/
Quante sono le stringhe binarie con 3 uni e 4 zeri?
$\binom{7}{3} \cdot 1$ e in effetti è uguale a $\binom{7}{4}$

4/
Quante sono le soluzioni $\{(x,y,z) \in \mathbb{N}^3 \mid x+y+z = 11\}$
consiste dare corrispondenza tra le triple e le stringhe binarie ad esempio
$(2,5,4) \longrightarrow$ 1 1 0 1 1 1 1 1 0 1 1 1 1
2 la virgola 5 4
Sono stringhe lunghe 13, con 11 uni.
Dunque $\binom{13}{11} = \frac{13!}{2!\,11!} = \frac{13 \cdot 12}{2!} = 13 \cdot 6 = 78$

5/
Quante anagrammi di anna?
Avendo sempre 5 caselle la soluzione è 5!
5 scelte, 3 scelte, 2 scelte, 1 scelta
Anagrammi di Mamma?
$\binom{5}{2} = \frac{5!}{3!\,2!} = \frac{5 \cdot 4}{2!} = 10$
0 1 0 0 1

Anagrammi di attillata? Li può fare in 2 modi
1) scelgo la posizione delle 2a $\binom{9}{2}$
2) scelgo la pos delle 3t $\binom{7}{3}$
3) " 2l $\binom{4}{2}$
4) " dell'unica I = 1

$\binom{9}{2} \cdot \binom{7}{3} \cdot \binom{4}{2} = \frac{9!}{7!\,2!} \cdot \frac{7!}{4!\,3!} \cdot \frac{4!}{2!\,2!} = \frac{9 \cdot 8}{2} \cdot \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} \cdot \frac{2}{2}$

~~= 1 36 35 16 2~~

$\frac{9!}{7!\,2!} \cdot \frac{7!}{4!\,3!} \cdot \frac{4!}{2!\,2!} = \frac{9!}{(2!)(3!)(2!)}$

n° delle a, n° delle t, n° delle l

regola generale

6/
Quante una scacchiera 3×3 con colorazioni binarie è nera.
1) In quanti modi posso colorarla? 2^3
2) Quante affinché ogni riga sia diversa? $2^3 \cdot (2^3-1) \cdot (2^3-2)$
3) $\exists$ una riga bianca? $3 \cdot (2^3-1) \cdot (2^3-1)$
4) $\exists$ una bianca = TUTTE − nessuna bianca $= 2^9 - (2^3-1)(2^3-1)(2^3-1)$
5) almeno una riga monocolore $= 2^9 - (2^3-2)(2^3-1)(2^3-2)$

- Binomio di Newton
la somma delle righe dell'n-esima riga è 2^n infatti:
$2^5 = (1+1)^5 = \sum_{i=0}^{5} \binom{5}{i} 1^i \cdot 1^{5-i}$

1/ compito

12/11/13.

Quante sono le funzioni che vanno da 20 a 20 cioè

$f:[20] \to [20]$ dove $[20] = \{1, 2, \dots, 20\}$

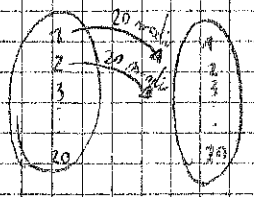
a) che assumono almeno un valore ≥ 11

Per complementare: TUTTE − (quelle

$= 20^{20} - |\{f \mid f:[20] \to [10]\}| =$

$= 20^{20} - 10^{20}$

Se non avessi restrizioni



sarebbero 20^{20}

b) che oppure assumano esattamente un valore ≥ 11

Scelgo innanzitutto in quanti modi posso scegliere un numero ≥ 11 Sono 10

Poniamo di scegliere il 13. Quante mi chiedo

Quante $f:[20] \longrightarrow [10] \cup \{13\} = 11^{20}$ da cui però devo sottrarne tutte

quelle in cui $13 \notin \mathrm{Im}(f)$. Esse sono 10^{20}. In conclusione:

$$10 \cdot (11^{20} - 10^{20})$$

↑ scelgo un valore ≥ 11

c) Quanti sono i sottoinsiemi di $[20]$ che contengono esattamente 3 pari

(e zero oppure più dispari)

$\binom{10}{3} \cdot (2^{10})$ ← n° delle P_{comp} cioè il numero di sottoinsiemi possibili contenenti dispari

↑ modi di scegliere i 3 numeri pari

Teorema: principio di inclusione esclusione

Presi due insiemi A, B allora

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Se ne ho 3 di insiemi:

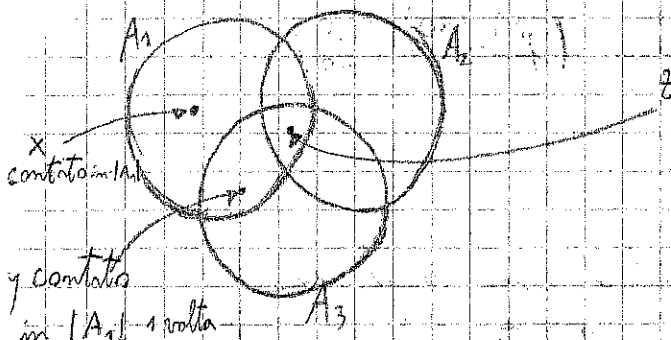
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

In generale se ho m insiemi avrò che:

$$|A_1 \cup \dots \cup A_m| = \sum_{\emptyset \neq I \subseteq \{1,\dots,m\}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} A_i \right|$$

Cerchiamo di dare una giustificazione del principio nel caso $n=3$ cioè

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3|$$



z l'ho contato
1 volta in $|A_1|$, 1 volta in $|A_2|$, 1 volta in $|A_3|$
-1 volta in $|A_1 \cap A_2|$, -1 volta in $|A_2 \cap A_3|$, -1 volta in $|A_3 \cap A_1|$
1 volta in $|A_1 \cap A_2 \cap A_3|$

Dunque l'ho contato $(1+1+1)-(1+1+1)+1=1$
L'ho dunque contato 1 volta.

Dunque in qualunque regione io scelga un elemento lo conto solo una volta. Non ho quindi problemi di doppio conteggio.

Esercizio: Quante sono $f: X \to [3]$ suriettive? Per complemento

TUTTE - non suriettive. Cioè:

$3^n - (P_1 \cup P_2 \cup P_3)$ con $P_i = \{f \mid f: [n] \to [3],\ i \notin \mathrm{Im}(f)\}$

Nel nostro caso stiamo parlando di TUTTE le funzioni a cui sottraggo:

1) quelle che "non coprono" 1
2) " " 2
3) " " 3

Ho che $P_1 = \{f \mid f: [n] \to \{2,3\}\}$ dunque $|P_1| = 2^n$

Lo stesso vale per P_2 e P_3. Ma devo considerare le ripetizioni. Tramite il principio di inclusione esclusione ho che

$$|P_1 \cup P_2 \cup P_3| = |P_1| + |P_2| + |P_3| - (|P_1 \cap P_2| + |P_2 \cap P_3| + |P_3 \cap P_1| - (|P_1 \cap P_2 \cap P_3|)) =$$

$$= 2^n + 2^n + 2^n - (1^n + 1^n + 1^n - (0^n)) = 3 \cdot 2^n - 3$$

Nel complesso: $3^n - (3 \cdot 2^n - 3) = 3^n - 3 \cdot 2^n + 3$

Esercizio 40 studenti in 4 classi 13/11/12

Classe 1, 2, 3, 4

a) In quanti modi se voglio 10 studenti per classe $\binom{40}{10}\cdot\binom{30}{10}\cdot\binom{20}{10}=$

$= \frac{40!}{30!10!}\cdot\frac{30!}{20!10!}\cdot\frac{20!}{10!10!} = \frac{40!}{(10!)^4}$

b) In quanti modi se gli studenti possono andare come vogliono

$f:[40]\to[4]$ dunque 4^{40} Cioè ogni studente ha 4 possibili scelte

c) Almeno uno studente per classe?

Devo contare le funzioni suriettive $f:[40]\to[4]$

Usando il complementare conto: TUTTE - non SURIETTIVE

Cioè $P_i = \{f \mid f:[40]\to[4],\ i\notin Im(f)\}$

La classe i resta vuota in 3^{40} modi (che sono il modo di disporre gli altri studenti nelle restanti aule.

Dunque $|P_1| = |P_2| = |P_3| = |P_4| = 3^{40}$

In conclusione

TUTTE - non SURIETTIVE $= 4^{40} - |P_1\cup P_2\cup P_3\cup P_4|$

Per il principio di inclusione esclusione:

$|P_1\cup P_2\cup P_3\cup P_4| = \sum_{i=1}^{4}|A_i| - \sum_{i<j}|P_i\cap P_j| + \sum_{i<j<k}|P_i\cap P_j\cap P_k| - |P_1\cap P_2\cap P_3\cap P_4|$

$= 4\cdot 3^{40} - \binom{4}{2}\cdot 2^{40} + \binom{4}{3}\cdot 1^{40} - 0$

Dunque $4^{40} - (4\cdot 3^{40} - \binom{4}{2}\cdot 2^{40} + \binom{4}{3}\cdot 1^{40})$

- Ripasso

1) n° di funzioni: $|\{f \mid f:[k] \to [n]\}| = n^k$

2) n° di funzioni iniettive: $|\{f \mid f:[k] \to [n]\}| = \begin{cases} 0 & \text{se } k > n \\ \frac{n!}{(n-k)!} & \text{se } k \leq n \end{cases}$

3) Quante sottoinsiemi $\binom{n}{k}$ di k elementi da n:

Ci chiediamo adesso quale differenza vi sia fra le stringhe e gli insiemi:

$(1,4,6,7) \neq (1,6,7,4)$ mentre $\{1,4,6,7\} = \{1,6,7,4\}$

Dunque presi n elementi ho meno insiemi che stringhe. Dunque

Scegliere una stringa $\frac{n!}{(n-k)!}$ = Scegliere l'insieme dei suoi elementi $\binom{n}{k}$ e poi disporli $k!$

Dunque deve essere che $\frac{n!}{(n-k)!} = \binom{n}{k} \cdot k! \implies \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$

- Formula di Stiefel

Preso il triangolo di Tartaglia:

0 1

1 1 1

2 1 2 1

3 1 3 3 1

Voglio dimostrare che $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ con $k > 0$

Dim: presi n elementi $\{1,2,\dots,n\}$ se scelgo k

Ho 2 possibilità:

1) Prendo n e altri $k-1$ elementi

2) Non prendo n e ne prendo altri k

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

sottoinsiemi in cui ho preso n

sottoinsiemi in cui non ho preso n

- Binomio di Newton

La si dimostra per induzione

- Triangolo di Tartaglia

```
                1
            1       1
        1       2       1
    1       3       3       1
1       4       6       4       1
    1       5      10      10       5       1
```

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

1 - 3 + 3 - 1

1 - 4 + 6 - 4 + 1 → questo invece mi sorprende ma lo so dimostra

1 - 5 + 10 - 10 + 5 - 1

$0 = (1-1)^n =$

- Aritmetica

Riprendiamo la divisione euclidea con resto

$n \mid k$ $\quad n = k \cdot q + r$

$r \mid q$ $\quad$ con $0 \leq r < k$

Cioè $\forall n, k$ con $k \neq 0$ $\exists!\ q, r \mid n = kq + r \wedge 0 \leq r < k$

Graficamente: 0 — k — 2k — ··· — qk — n — (q+1)k

Prendiamo $65 \mid 7$ $\quad 2 \mid 9$ $\quad -65 \mid 7$ $\quad +5 \mid -10$

- Congruenza (in $\mathbb{Z}$) 19/11/13

$a \equiv b \ (c) \iff c \mid a-b$ cioè $\exists k$ tale che $ck = a-b$

Cioè a è congruo a b modulo di c se c divide a-b

esempio: $x \equiv 0 \ (12) \iff 12 \mid x$ (12 divide x) cioè $\exists k \ 12k = x$

Teorema banalità: $a \equiv b \ (c) \iff$ a e b danno stesso resto diviso 12

esempio 2: $15 \equiv 3 \ (12)$ infatti se faccio la divisione intera di 15 ho resto 3. lo stesso vale se faccio la divisione intera di 3

esempio 3: trovare il resto di $(12^5 3^4 2^3 \cdot 13^4 4^3 2)$ mod 5

Il "trucco" è che non mi conviene moltiplicarli e trovare il resto, ma fare il contrario: $12^5 3^4 2^3$ mod 5 = resto 3 $\quad 13^4 4^3 2$ mod 5 = resto 2

Dunque il resto sarà $3 \cdot 2 = 6$ cioè 6 mod 5 = 1

Potrei anche scrivere il resto in diversi modi

esempio 3: $11 = 4\cdot 2 + 3$ oppure $11 = 4\cdot 3 - 1$ oppure $11 = 4\cdot 1 + 7$

In generale si tende a privilegiare il resto positivo e minore del modulo. Nel nostro esempio dunque, il primo modo che abbiamo scritto

esempio 4: $2^{99} \bmod 7$?

Infatti $2^{99} = 2^{3\cdot 33} = (2^3)^{33} \equiv (1)^{33} \equiv 1\ (7)$

abbiamo quindi implicitamente detto che

$a \equiv b\ (c) \Rightarrow a^n \equiv b^n\ (c)$

esempio 5: $3^{11} \bmod 5$?

$3^{11} = 3^2 \cdot 3^2 \cdot 3^2 \cdot 3^2 \cdot 3^2 \cdot 3$

ma poiché $3^2 = 9 \underset{5}{\equiv} 4 = -1\ (5)$ ma dunque

$3^{11} = (3^2)^5 \cdot 3 \underset{5}{\equiv} (-1)^5 \cdot 3 \equiv -1 \cdot 3 \equiv -3 \equiv 2\ (5)$

Anche qui abbiamo implicitamente detto che

se $\begin{cases} a_1 \equiv b_1\ (c) \\ a_2 \equiv b_2\ (c) \end{cases} \Rightarrow a_1 \cdot a_2 \equiv b_1 b_2\ (c)$

Sopra infatti abbiamo scritto che

$$\begin{cases} 9 \equiv -1\ (5) \\ 9 \equiv -1\ (5) \\ 3 \equiv 3\ (5) \end{cases} \Rightarrow 3\cdot 9 \cdot 9 \equiv (-1)\cdot(-1)\ (c)$$

esempio 6: Vediamo alcune "prove di divisibilità"

Consideriamo il numero $1234567 = 1\cdot 10^6 + 2\cdot 10^5 + 3\cdot 10^4 + 4\cdot 10^3 + 5\cdot 10^2 + 6\cdot 10 + 7$

Resto per 3 e per 9

$10 \underset{3}{\equiv} 1$ dunque al posto dei 10^n posso scrivere 1 dunque

$1234567 \underset{3}{\equiv} 1+2+3+4+5+6+7 \underset{3}{\equiv} \cancel{1+2} + \cancel{4+5} + 7 \underset{3}{\equiv} 7 \underset{3}{\equiv} 1$

Vediamo adesso se 1234567 dà resto nullo oppure no se diviso per 11

$1234567 \equiv 1\cdot(-1)^6 + 2(-1)^5 + 3(-1)^4 + 4(-1)^3 + 5(-1)^2 + 6(+1)^1 + 7$

$\underset{11}{\equiv} 1 - 2 + 3 - 4 + 5 - 6 + 7 \underset{11}{\equiv} 4$

Poiché $10 \bmod 11 = -1$

Vediamo il resto di $1234567 \bmod 4$

$1234567 = 10^2(1\cdot 10^3 + 2\cdot 10^3 + 3\cdot 10^2 + 4\cdot 10 + 5) + 67 \underset{4}{\equiv} 0 + 67 \underset{4}{\equiv} 3$

poiché $100 \bmod 4 = 0$

Vediamo il resto di $1234567 \bmod 7$

Diciamo che $1000 = 7\cdot 143 - 1$. Dunque $1000 \equiv -1 \ (7)$

$1234567 = 1\cdot 1000^2 + 234\cdot 1000 + 567 \underset{7}{\equiv} (-1)^2 + 234\cdot(-1) + 567 = 334 \underset{7}{\equiv} 5$

Esempio 7: Sapendo che $\sqrt{1234567}$ non è intera, cerchiamo per assurdo che sia intera. Dunque per assurdo sia $x \in \mathbb{N}$ $x^2 = 1234567$

Partendo dall'assunto che se due numeri sono uguali allora sono anche congrui in qualunque modulo

Prendiamo allora (poiché $x^2 = 1234567$)

$x^2 \underset{3}{\equiv} 1234567 \equiv 1$

Questo non ci porta ad alcuna contraddizione.

Proviamo allora

$x^2 \underset{4}{\equiv} 1234567 \underset{4}{\equiv} 3$

$0^2 \equiv 0 \ (4)$ $\quad 3^2 \equiv 1 \ (4)$ $\quad 6^2 \equiv 0 \ (4)$

$1^2 \equiv 1 \ (4)$ $\quad 4^2 \equiv 0 \ (4)$

$2^2 \equiv 0 \ (4)$ $\quad 5^2 \equiv 1 \ (4)$

Possiamo ripetere sempre i primi 4 casi poiché ad esempio

$5 \underset{4}{\equiv} 1$ e $5^2 \underset{4}{\equiv} 1^2$

$1010 \underset{4}{\equiv} 2$ e $(1010)^2 \underset{4}{\equiv} 2\cdot 2 = 4 \underset{4}{\equiv} 0$

Questo avviene poiché io posso scrivere ogni numero come uno dei primi 4 a cui aggiungo un multiplo di 4.

In particolare $x^2 = 1234567$ non può essere quadrato perché non può essere che $x^2 \underset{4}{\equiv} 3$. Cioè un assurdo

Esempio 8: Vediamo di risolvere una equazione contenente una congruenza

$6X \equiv 7 \ (29)$?

Abbiamo avvalendoci del fatto che TEO: $a \equiv b \ (c) \Rightarrow ka \equiv kb \ (c)$

dim: $a = b + nc \Rightarrow ka = kb + kn c$

Riprendiamo $6X \equiv 7 \ (29) \Rightarrow 5 \cdot 6X \equiv 5 \cdot 7 \ (29) \rightarrow 30X \equiv 35 \ (29) \rightarrow X \equiv 6 \ (29)$

Dunque $x = 6$. Infatti sostituendo 6 nella formula iniziale ottengo un'identità

Teorema: $a \equiv b \ (c) \iff a + n \equiv b + n \ (c)$

dim: $a \equiv b \ (c) \iff c \mid a - b$ preso allora $a + n \equiv b + n \ (c) \iff c \mid (a+n) - (b+n) = a + b$

Definizione: b è inverso di a modulo $c \iff b \cdot a \equiv 1 \ (c)$

Esempio 9: $5 \cdot 6 \equiv 1 \ (29)$ 5 e 6 sono uno inverso dell'altro mod 29

Esempio 10: $5X \equiv 1 \ (14) \Rightarrow 15X \equiv 3 \ (14) \rightarrow 1X \equiv 3 \ (14)$ dunque $x = 3$ è soluzione ma anche $x = 3 + k \ (14)$

Esempio 11: $15X \equiv 7 \ (25)$

Questa non ha soluzione perché $15x = 7 + k \cdot 25$ Poiché $15x$ è multiplo di 5 e anche $25k$ ma poiché $25k + 7$ NON può essere multiplo di 5 allora $15x$ non può essere uguale a $25k + 7$. Dunque non esiste soluzione

Esempio 12: $70X \equiv 14 \ (58) \iff 12X \equiv 14 \ (58)$ inoltre sono tutti divisibili per 2

$6X \equiv 12X \equiv 14 \ (58) \Rightarrow 6X = 7 + 29k \iff 6X \equiv 7 \ (29) \Rightarrow$

$\Rightarrow 5 \cdot 6X \equiv 5 \cdot 7 \ (29) \rightarrow 30X \equiv 35 \ (29)$ dunque $x = 6$

• Massimo comun divisore

20/11/13

$\exists x [a x = b \cdot c)] \iff MCD(a,c) \mid b$

Che cosa è il massimo comun divisore? Vediamolo tramite un esempio

esempio 1: MCD (252, 198) è il numero più grande possibile che divide sia 252 che 198. Scomponiamo i due numeri in fattori

$252 = 2^2 \cdot 3^2 \cdot 7$
$198 = 2 \cdot 3^2 \cdot 11$
$\Rightarrow 2 \cdot 3^2 = 18 = MCD(252, 198)$

↳ sono tutti quelli in comune tra 252 e 198

Questo metodo non è particolarmente comodo per grandi numeri. Vediamo un altro metodo

Esempio 2: $MCD(252, 198) = MCD(198, 54) = MCD(54, 36) = MCD(36, 18) = 18$

$252 = 198 \cdot 1 + 54$
$198 = 54 \cdot 3 + 36$
$54 = 36 \cdot 1 + 18$
$36 = 18 \cdot 2 + 0$

In generale vale che $MCD(a, b) = (a, b-a)$ Se definiamo $b = aq + a$ possiamo allora sottrarre "a" per q volte da b se $b > a$

Dunque $(a, b - qa) \rightarrow$ resto di b diviso a

$= (a, b \bmod a)$

Vale anche che "x divide sia b che a $\iff$ x divide a e b-a" Dunque che $\{x : x \mid a \wedge x \mid b\} = Divisori(b, a) = Divisori(a, b-a)$ dimostriamolo:

$\Rightarrow x \text{ div } (b, a) \Rightarrow \exists k \; b = kx \Rightarrow b - a = (k - k')x$
$\exists k' \; a = k'x$

$\Leftarrow x \text{ div } (a, b-a) \Rightarrow \exists k \; xk = a \Rightarrow b = x(k + k')$
$\exists k' \; xk' = b - a$

Teorema di Bezout

Dati $a, b \in \mathbb{Z}$ con $a \neq 0 \vee b \neq 0$, esiste $d = MCD(a,b)$ cioè:

$\exists x,y \; [d = ax + by]$

Esempio: negli esempi visti prima $MCD(252, 198) = 18$ cioè $\exists x,y \; 18 = 252x + 198y$

cioè $252x \equiv 18 \pmod{198}$ } sono risolvibili grazie
$198y \equiv 18 \pmod{252}$ } al teorema di Bezout

Dimostriamo il teorema di Bezout partendo dal caso particolare $MCD(252, 198)$

Esempio 2: Partiamo dai numeri dell'algoritmo di Euclide

$252 = 252 \cdot [1] + 198\,[0]$ Cerchiamo quei valori che moltiplicati per

$198 = 252\,[0] + 198\,[1]$ 252 e 198 rispettino l'equazione

$252 - 198 = 54 = 252\,[1] + 198\,[-1]$ } coeff. sono ricavati come segue: $36 = 198 - 54 \cdot 3$

$198 - 54 \cdot 3 = 36 = 252\,[-3] + 198\,[4]$ Prendo 1 volta i coeff di 198 e gli sottraggo quelli

$54 - 36 = 18 = 252\,[4] + 198\,[-5]$ di 54 moltiplicati per 3: $1 \cdot (0,1) - 3 \cdot (1,-1) = (-3, 4)$

Abbiamo trovato che una soluzione di $18 = 252x + 198y$ è $x = 4$, $y = -5$

Ce ne sono altre? Sì. Infinite perché mi basta scrivere $x = 4 + 198 \cdot k$

e $y = -5 - 252 \cdot k$ ad esempio

$x = 4 + 198$, $y = -5 - 252$ e si verifica che è soluzione.

Ma in tal modo le abbiamo trovate tutte? NO!

Proviamo a cercarle:

$18 = 252x + 198y \longrightarrow 1 = 14x + 11y$ Adesso possiamo procedere

come prima:

$\begin{cases} x = 4 + k \cdot 11 \\ y = -5 - k \cdot 14 \end{cases}$ Queste sono TUTTE le soluzioni (sono in effetti molto più "fitte")

Verifichiamolo tramite Bezout

Esempio 3: $1 = 14x + 11y$ $(14, 11)$

$14 = 11 \cdot 1 + 3$ $(14, 11)$

$11 = 3 \cdot 3 + 2$ $(11, 3)$

$3 = 2 \cdot 1 + 1$ $(3, 2)$

$2 = 1 \cdot 2 + 0$ $(2, 1) = 1$

	14	11
14	1	0
11	0	1
$14 - 11 = 3$	1	-1
$11 - 3 \cdot 3 = 2$	-3	4
$3 - 2 = 1$	4	-5

Queste questioni sono legate alla questione dell'inverso. In effetti da $1 = 14 \cdot 4 \ (11)$ ricavo che 14 e 4 sono inversi l'uno dell'altro modulo 11

esempio 4: $1 \equiv 11(-5) \ (14)$

$1 \equiv 11 \cdot 9 \ (14)$

esempio 5: Risolvere $14x \equiv 1 \ (11)$ la moltiplichiamo per l'inverso di 14 (che è 4)

$4 \cdot 14x \equiv 4 \ (11)$

$x \equiv 4 \ (11)$

Ma allora mi basta trovare le soluzioni di $x \equiv 4(11)$ cioè le infinite soluzioni sono $x \equiv 4 + k \cdot 11$

In generale possiamo chiederci quali siano le soluzioni di $n = ax + by$ con n, a, b noti. Facciamo qualche altro esempio

esempio 6: $72 = 252x + 198y$ la possiamo risolvere perché 72 è multiplo di 18

Infatti se $18 = 252 \cdot (4) + 198(-5)$ allora $72 \equiv 252 \cdot (4 \cdot 4) + 198 \cdot (-5 \cdot 4)$

Scritta nella forma: $252x \equiv 72 \ (198)$ posso dire che, siccome $MCD(252, 198) = 18$ divide 72 allora è risolubile

Se io la volessi risolvere scriverei:

$252x \equiv 72 \ (198) \iff 14x \equiv 4 \ (11) \iff 3x \equiv 4 \ (11) \iff 4 \cdot 3 \equiv 16 \ (11) \iff$

$\iff x \equiv 16 \ (11) \iff x \equiv 5 \ (11)$ cioè $x = 5 + k \cdot 11$

Dimostriamo adesso il teorema di Bezout

* (Il minimo CL (non a, b) = (Massimo intero che divide sia a che b))

Chiamiamo "combinazione lineare" di (a, b): $CL(a,b) = \{\overset{\circ}{n} \mid \exists x, y \ \ n = ax + by\}$

Consideriamo il minimo tra gli elementi che rispettano l'equazione. Prendiamo $m \mid a$. m divide a se $a = m \cdot q + r$ dove m è il nostro minimo.

$m = ax_0 + by_0$ dunque $a = ax_0 q + by_0 q + r$ dunque $r = a(1 - x_0 q) + b(-y_0 q)$

Dunque $r \in CL(a,b)$ dove r deve essere zero poiché $0 \leq r < m$, ma m era il più piccolo. Con lo stesso ragionamento si dimostra che $m \mid b$. Quindi m è divisore di a e di b. Ma è il massimo? Prendiamo un altro divisore h di "a" e di "b"

È dunque $h \mid CL(a,b)$ e dunque $h \mid m$. Ma poiché $h \mid m$ allora $h \leq m$. Dunque,

26/11/13

- Conseguenze di Bezout

Presi $a, b, n \in \mathbb{Z}$ allora $\exists x, y \in \mathbb{Z} : n = ax + by \iff MCD(a,b) \mid n$

$\Rightarrow$ facile perché risolta $n = ax + by$ diviene facile dimostrare che se $MCD(a,b) \mid n$ perché divide a ~~MCD~~ divide anche b e la loro somma dunque divide n

esempio $\exists x y \quad 17 = 252x + 198y$ NO! perché

$2 \mid 252 \quad 2 \mid 198 \Rightarrow 2 \mid 252x \Rightarrow 2 \mid 252x + 198y \Rightarrow 2 \mid 17$ che è assurdo

esempio 2: presi $a, b, c \in \mathbb{Z}$ ~~$\forall \exists \in$~~ tali che

$a \mid bc \Rightarrow a \mid b \vee a \mid c$?

$6 \mid 2 \cdot 3$ ma $6 \nmid 2$ e $6 \nmid 3$

$6 \mid 4 \cdot 9$ ma $6 \nmid 4$ e $6 \nmid 9$

dunque in generale NO

Però se a è primo allora sì

- Teoremi

(a) Se $a \mid bc$ e $MCD(a,b) = 1 \Rightarrow a \mid c$

dim uso bezout $\Rightarrow \exists x, y \in \mathbb{Z} \quad 1 = ax + by \Rightarrow c = acx + bcy$

$a \mid bc$ per ipotesi dunque $a \mid bcy$ è multiplo di a e di acx. La loro somma dunque è divisibile per a dunque c è multiplo di a. Cioè $a \mid c$

(b) somma di 2 multipli di a è multiplo di a

dim $a \mid m_1 \quad a \mid m_2 \Rightarrow a \mid m_1 + m_2$

$\Downarrow \quad \Downarrow$

$m_1 = ax \quad m_2 = ay \Rightarrow m_1 + m_2 = ax + ay = a(x+y)$

(c) Se p è primo (cioè $p > 1$ e $p = a \cdot b \Rightarrow a = \pm 1 \vee a = \pm p$) e $p \mid ab \Rightarrow p \mid a \vee p \mid b$

Suppongo che $p \mid ab$. Voglio dimostrare $p \mid a \vee p \mid b$. Suppongo allora $p \nmid a$ e mostro che $p \mid b$.

Poiché p è primo e $p \nmid a$ allora $MCD(p,a) = \begin{cases} 1 \\ \cancel{p} \end{cases} \Rightarrow \exists x, y \in \mathbb{Z} \quad 1 = px + ay$

ma ne segue $b = pbx + aby$ ma poiché sia pbx è multiplo di p e anche aby lo è, allora $p \mid b$

• Divisione nelle congruenze

Preso $14 \equiv 8 \ (6)$ posso dire che

$7 \equiv 4 \ (6)$? NO ho diviso soltanto 14 e 8 per 2

$7 \equiv 4 \ (3)$? SI ho diviso tutto per 2

• Teorema

$ac \equiv bc \ (nc) \iff a \equiv b \ (n)$

(a) dim: $\exists k \ ac = bc + kn \Rightarrow \exists k \ a = b + kn$ cioè $a \equiv b \ (n)$

(b) Se $a \cdot c \equiv bc \ (n)$ e $MCD(c, n) = 1$ allora $\Rightarrow a \equiv b \ (n)$

dim: da (1) $\iff n \mid ac - bc \iff n \mid c(a-b) \underset{MCD(c,n)=1}{\iff} n \mid a-b \iff a \equiv b \ (n)$

Esempio: $7x \equiv 14 \ (5)$ trovare tutte le x con $0 \leq x \leq 100$ che risolvono

Lo facciamo in 2 modi

1) $2x \equiv 4 \ (5)$ moltiplico per l'inverso di 2 (che è 3)

$x \equiv 12 \ (5)$ dunque $x \equiv 2 \ (5)$ e quindi $x = 2 + 5 \cdot k$ è soluzione.

Per sapere quante sono devo risolvere

$0 \leq 2 + 5 \cdot k \leq 100$ cioè $-\frac{2}{5} \leq k \leq \frac{98}{5}$ dunque poiché $k \in \mathbb{N}$ $0 \leq k \leq 19$

sono 20 soluzioni

2) Usando la divisione nelle congruenze

dico che $7x \equiv 14 \ (5) \iff x \equiv 2 \ (5)$ perché $MCD(7, 5) = 1$

• Inverso modulo m

def: Se $a \cdot b \equiv 1 \ (m)$ dico che "a e b" sono uno inverso dell'altro

Esiste un inverso di $a \bmod (m) \iff MCD(a, m) = 1$

dim: ($\Leftarrow$) supponiamo $MCD(a, m) = 1$, per Bezout $\exists x, y \in \mathbb{Z} \ 1 = ax + my \Rightarrow 1 \equiv ax \ (m)$

cioè x è inverso

($\Rightarrow$) se esiste l'inverso di $a \bmod m \Rightarrow MCD(a, m) = 1$; sia $\overset{x}{\cancel{x}}$ l'inverso di $a \bmod m$. cioè $a \cdot \overset{x}{\cancel{x}} \equiv 1 \ (m)$ cioè $1 = aX + my$. Dunque $1 \in CL(a, m)$ dunque $MCD(a, m) = 1$

• Classi resto

Presi $a, b \in \mathbb{Z}$ e preso $m \in \mathbb{Z}$ $\quad [a]_m = \{c \mid c \equiv a\ (m)\}$

Esempio: $[2]_5 = \{2, 7, 12, \dots, -3, -8, \dots\} = [7]_5$

cioè $a \equiv b\ (m) \iff [a]_m = [b]_m$. Dunque in $[\,]_m$ esistono m classi di resto

Esempio 2: $[0]_5 = [5]_5 = \dots$ In questo esempio ho soltanto 5 classi di resto possibili

$[1]_5 = [6]_5 = \dots$

$[2]_5 = [7]_5 = \dots$

$[3]_5 = [8]_5 = \dots$

$[4]_5 = [9]_5 = \dots$

Notiamo che preso p primo tutti i numeri $1, 2, 3, \dots, p-1$ hanno inverso mod p $\quad x \not\equiv 0\ (p)$

$MCD(x, p) = \begin{cases} \not{x} \\ 1 \end{cases}$ p non può essere perché allora dividerebbe x cioè $x \equiv 0\ (p)$

ottenendo 1 come soluzione $\Rightarrow$ esiste inverso di x mod p

27/11/13

Teorema

a) presi $a, b \in \mathbb{Z}$ (non entrambi 0) detto $d = MCD(a,b)$ si ha che

$MCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

b) $aX \equiv b\ (c)$ ha soluzione $\iff MCD(a,c) \mid b$

dim: ($\Rightarrow$) Supponga $d \mid b$. Divido tutto: $aX \equiv b\ (c) \iff \left(\frac{a}{d}\right) X \equiv \left(\frac{b}{d}\right)\ \left(\frac{c}{d}\right)$

con $\frac{a}{d} = a'$, $\frac{b}{d} = b'$, $\left(\frac{c}{d}\right) = c'$ dunque $a'X \equiv b'\ (c')$ e dunque MCD

$MCD(a', c') = 1 \Rightarrow$ esiste l'inverso di a' mod c. Chiamo u: $a'u = 1\ (c)$

$a'x \equiv b'\ (c')$

$ua x \equiv ub'c'$

$x \equiv ub'\ (c')$

$x = ub' + kc'$

($\Rightarrow$) $\exists x\ [aX \equiv b\ (c)] \Rightarrow \exists x\ \exists y\ \ b = ax + cy$ Quindi $b = ax + cy$ ha soluzione; per Bezout b è multiplo del $MCD(a,c)$ ovvero $MCD(a,c) \mid b$

1/es Berardinelli classe

$435X \equiv 15 \pmod{102} \iff 27X \equiv 15 \pmod{102} \iff 9X \equiv 5 \pmod{34}$

ma adesso $MCD(9,34) = 1$ Allora mi basta da trovare l'inverso di 9. Per farlo devo risolvere:

$9u \equiv 1 \pmod{34} \to 1 = 9u + 34y$ si può fare in due modi

a) $34 = 9 \cdot 3 + 7$

$9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1$

$2 = 1 \cdot 2 + 0$

	34	9
34	1	0
9	0	1
7	1	-3
2	-1	4
1	4	-15

Dunque $1 = (4)34 + 9 \cdot (-15)$ e quindi

$1 \equiv 9 \cdot (-15) \pmod{34}$

$1 \equiv 9 \cdot (19) \pmod{34}$

d'inverso è dunque 19

$9X \equiv 5 \pmod{34}$

$19 \cdot 9X \equiv 5 \cdot 19 \pmod{34}$ e dunque $x = 29 \pmod{34}$

b) $9X \equiv 5 \pmod{34} \iff 9X \equiv 5 - 2 \cdot 34 \pmod{34} \iff 9X \equiv -63 \pmod{34} \iff X \equiv -7 \pmod{34}$

posso dividere perché so che esiste il suo inverso (altrimenti non potrei)

e dunque $X = -7 + 34 \cdot 1 = 27$

2/es Berardinelli classe

$22X \equiv 12 \pmod{40}$

$11X \equiv 6 \pmod{20} \iff 11X \equiv 6 + 20 \cdot 3 \pmod{20} \iff 11X \equiv 6 \cdot 6 \pmod{20} \iff X \equiv 6 \pmod{20}$

- Numeri primi
- Teorema

Esistono infiniti primi

Dim (Euclide): supponiamo per assurdo che ne esista un numero finito $(p_1, p_2, \dots, p_N)$

chiamato $m = p_1 + \dots + p_N$ consideriamo $(m+1) = (p_1 + \dots + p_N + 1)$

In questo numero possiamo dire che $(m+1) \equiv 1 \bmod p_i$

Ma poiché esiste sempre $q \mid (p_1 \dots p_N + 1)$ dove q deve essere primo (TEO già dimostrato) se un numero non è primo allora è divisibile per un primo e poiché $q \neq p_1 \dots p_N$ allora q è un nuovo primo.

1/ es Berardocci classe

Quanti sono i divisori di 8000?

Gli unici primi che la fanno sono 2 e 5. Ad esempio $7 \nmid 8000$ perché vanno nelle varie che $7 \mid 8000 \Rightarrow 7 \mid 2^6 \vee 7 \mid 5^3 \equiv 7 \mid 2 \vee 7 \mid 5$

Divisori di 8000 sono scrivibili come $2^a \cdot 5^b$ dove $a \leq 6$, $b \leq 3$

Dunque posso scegliere a in 7 modi e b in 4 modi. Dunque $7 \cdot 4 = 28$ modi

- Sistemi di congruenze 3/12/13

$$\begin{cases} aX \equiv b \ (m) & (i) \\ a'X \equiv b' \ (m') & (ii) \end{cases}$$ voglio la x che risolve simultaneamente (i) e (ii)

In generale si trovano le soluzioni di una e si inseriscono nell'altra per vedere se vanno bene

Portato il sistema nella forma

$$\begin{cases} X \equiv d \ (c) \\ X \equiv d' \ (c') \end{cases}$$ ← ha soluzioni $MCD(c, c') \mid d - d'$

esempio: $\begin{cases} X \equiv 3 \ (6) & X = 3, 9, 15, \dots, -3, \dots \\ X \equiv 4 \ (8) & X = 4, 12, \dots, -4 \end{cases}$

non ha soluzioni perché $MCD(6,8) \nmid 4-3$

Se per assurdo un valore $x = n \in \mathbb{Z}$ risolvesse il sistema allora

$n \equiv 3 \ (6) \Rightarrow n \equiv 3 \ (2)$ $\Rightarrow$ assurdo perché n è congruo sia a 3 che a 4

$n \equiv 4 \ (8) \Rightarrow n \equiv 4 \ (2)$

- Metodo di risoluzione

$$\exists X \begin{cases} X \equiv a \ (m) \\ X \equiv a' \ (m') \end{cases} \iff MCD(m, m') \mid (a - a')$$

$$\iff a \equiv a' \ (MCD(m, m'))$$

esempio: $\begin{cases} X \equiv 13 \ (21) & (i) \\ X \equiv 16 \ (45) & (ii) \end{cases}$ $\exists x$? $MCD(21, 45) = 3 \mid 16 - 13 = 3$ SI'

(i) ha soluzione $x = 13 + 21k$ Sostituisco in (i) e vedo se mi ramollene l'una soluzione:

$(*) \to 13 + 21k \equiv 16 \ (45)$ proviamo allora a risolvere (perché se k è soluzione dell'equazione, allora è soluzione del sistema)

$(\star)$ $21k \equiv 3 \ (45)$

$7k \equiv 1 \ (15)$ L'inverso esiste perché $MCD(7,15) = 1$ Lo possiamo trovare tramite Bezout risolvendo: $1 = 7u + 15v$

$2 \cdot 7 \equiv 14 \equiv -1 \ (15)$

$(-2) \cdot 7 \equiv 1 \ (15)$

Dunque -2 è l'inverso di 7 Allora posso scrivere

$-2 \cdot 7k \equiv -2 \cdot 1 \ (15)$

$k \equiv -2 \ (15)$

Dunque le soluzioni sono $k = -2 + 15l$

Adesso oppiamo che $x = 13 + 21k$ risolve la prima. Ma sostituendo k:

$x = 13 + 21(-2 + 15l) = -29 + 315l$ dunque $x = -29 \ (315)$

Non è un caso che il modulo del risultato sia 315. Infatti $mcm(21,45) = 315$

- Teorema

$\begin{cases} X \equiv a \ (m) \\ X \equiv a' \ (m') \end{cases}$ ha soluzione $\iff MCD(m,m') \mid a - a'$

Se esiste una soluzione x_0 le altre sono $x_0 + k \, mcm(m,m')$ dunque

$X \equiv qualcosa \ (mcm(m,m'))$

Inoltre se $MCD(m,m') = 1 \implies$ c'è sempre soluzione

Esempio 2: $\begin{cases} X \equiv 1 \ (60) \\ X \equiv 1 \ (24) \end{cases}$ qui sicuramente abbiamo soluzione perché $MCD(60,24) \mid 1-1$

$mcm(60,24) = \frac{60 \cdot 24}{MCD(60,24)} = \frac{60 \cdot 24}{12} = 120$

Quindi le soluzioni del sistema saranno sicuramente in modulo 120. In questo caso la soluzione è banale. Si vede che $x \equiv 1$ risolve. Detto ciò, vista che sappiamo la periodicità delle soluzioni scriviamo $x \equiv 1 \ (120)$

Esempio 3: (*) $19X \equiv 12 (35)$ potremmo risolverla singolarmente ma poiché sappiamo che $35 = mcm(7,5)$ possiamo riscriverla come

$$\begin{cases} 19X \equiv 12 (5) & (i) \\ 19X \equiv 12 (7) & (ii) \end{cases}$$

Dimostriamo che la possiamo fare:

(i) + (ii) $5 \mid (19X-12) \wedge 7 \mid (19X-12) \iff 35 \mid (19X-12)$ poiché se $5 \mid a \wedge 7 \mid a \iff 35 \mid a$

(*) dice che $35 \mid a$

(i) + (ii) dice che $5 \mid a \wedge 7 \mid a$

Stanno dunque dicendo la stessa cosa

Risolviamo allora il sistema

$$\begin{cases} 19X \equiv 12 (5) \\ 19X \equiv 12 (7) \end{cases} \begin{cases} -X \equiv 2 (5) \\ -2X \equiv -2 (7) \end{cases} \begin{cases} X \equiv -2 (5) \\ X \equiv 1 (7) \end{cases}$$

Dove nell'ultimo passaggio in (ii) ho diviso per -2 perché $MCD(-2,7) = 1$

Ora sappiamo che vi è soluzione perché $MCD(5,7) = 1 \mid -3$

ad occhio troviamo le soluzioni.

Da (ii) vedo che $X \equiv 1 (7) \Rightarrow X = 1, 8, 15, 22, 29$ e tra di esse vi deve sicuramente essere una soluzione poiché tra $0 < x < 35$ x è soluzione

Ma da (i) vedo che $X \equiv -2 (5) \Rightarrow X = 3, 8, 13, 18, 23, 28, 33$.

Il valore 8 è comune ad entrambe dunque $X \equiv 8 (35)$ che è la soluzione dell'equazione

- Congruenze esponenziali

$2^x \equiv 4 (7)$ però se trovo una soluzione (nell'esempio, $x=2$) non è vero che $2+7$ sia soluzione.

Il piccolo teorema di Fermat: preso p primo $\Rightarrow a^p \equiv a (p) \Rightarrow a^{p-1} \equiv 1 (p)$ dove ho diviso se $MCD(a,p)=1$ cioè se $a \neq 0 (p)$ (non posso cioè dividere per 0)

$2^6 \equiv 1 (7)$ per il teorema di Fermat

Dunque riprendendo $2^x \equiv 4 (7)$

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
mod 7	1	2	4	1	2	4	1	2

dunque $2^x \equiv 4 \ (7)$ "ogni 3 valori"

dunque $x \equiv 2 \ (3)$ è soluzione

2, 3, 5 sono primi e dunque

1	2	1				
1	3	3	1			
1	4	6	4	1		
1	5	10	10	5	1	

$\binom{2}{2}$ $\binom{3}{2}$ $\binom{5}{2}$ $\binom{5}{5}$ 5 | 5, 10

- Teorema

(a) Se p è primo e $0 < i < p \Rightarrow p \mid \binom{p}{i}$

Ad esempio $\binom{5}{2}$ è multiplo di 5. Intuitivamente, da tartaglia

dim: $\binom{p}{i} = \frac{p!}{(p-i)!\,i!}$ ma allora $\binom{p}{i} \cdot (p-i)!\, i! = p!$

$p \mid p!$ sì $\Rightarrow p \mid \binom{p}{i} \underbrace{(p-i)!\, i!}_{\text{prodotti di n° } < p} \Rightarrow p \mid \binom{p}{i}$

$(p-i)!$ in sé non è detto che sia minore di p. Ma $(p-i)! = (p-i) \cdot (p-i-1) \dots (1)$ dunque sono molti fattori ed ognuno di essi è più piccolo di p

4/12/13

(b) lemma: se p è primo $(x+y)^p \equiv x^p + y^p \ (p)$

dim $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = \binom{p}{0} y^p + \underbrace{\dots + \binom{p}{i} y^{p-i} x^p + \dots}_{\equiv 0 \bmod p} + \binom{p}{p} x^p$

cioè "sopravvivono" solo il primo e l'ultimo termine

teorema $a^p \equiv a \ (p)$ dove p è primo

dim: Induzione su a $(a > 0)$

Caso base: $0^p = 0 \equiv 0 \ (p)$

Caso induttivo: supposto vero per a, lo dimostriamo per $(n+1)^p$

Dunque $(n+1)^p$ per il lemma $(n+1)^p \equiv n^p + 1^p \equiv n^p + 1$ ma per ipotesi induttiva $n^p + 1 \equiv n + 1$ Dunque $(n+1)^p \equiv n+1 \ (p)$

• Potenze modulo n

Riprendiamo l'esempio iniziale: $2^n \equiv ?\ (7)$

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

Facciamone un altro: $2^n \equiv ?\ (10)$

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
1	2	4	8	6	2	4	8	6

Anche qui abbiamo periodicità dei resti

• Teoremi

ⓐ Per ogni a, m esistono $i<j$ $a^i \equiv a^j\ (m)$

dim: I resti modulo m di $a^0, a^1, a^2, \dots$ non possono essere infiniti (più precisamente sono $<m$) quindi esistono due resti uguali. Cioè $\exists\ i<j\ a^i \equiv a^j\ (m)$

Corollario: dopo che ho avuto lo stesso per una volta, i successivi saranno gli stessi già incontrati in precedenza.

ⓑ Se $(a,m) \Rightarrow \exists\ i\ a^i \equiv 1\ (m)$

dim: $\exists\ i,j\ (i<j \wedge a^i \equiv a^j\ (m)) \Rightarrow 1 \equiv a^{j-i}\ (m)$

• Esponenti negativi

Supponiamo che $(a,m)=1$ esiste a^{-1} dove $a^{-1}\cdot a \equiv 1\ (m)$

esempio: $(3,10)=1$ $3^{-1}=7$ perché

3^0	3^1	3^2	3^3	3^4
1	3	9	7	1
		-1		$3^3\cdot 3$

dunque $3^{-4} = (3^{-1})^4 = 7^4\ (10)$

Possiamo anche dire che $a^{-n} \equiv (a^{-1})^n \equiv (a^n)^{-1}$

esempio: $[2^{-5}]_7 = [(2^5)^{-1}]_7 = [4^{-1}]_7 = [2]_7$ dunque $2^{-5} \equiv 2\ (7)$

Infatti $a^{-1}\cdot a \cdot a^{-1}\cdot a \cdot a^{-1}\cdot a \equiv 1\cdot 1\cdot 1 \equiv 1\ (m)$

ma anche $a^{-1}\cdot a^{-1}\cdot a^{-1}\cdot a\cdot a\cdot a \equiv 1\ (m)$ e dunque $a^{-3}\cdot a^3 \equiv 1\ (m)$

• Ordine di $a \in \mathbb{Z}$ modulo m = il minimo $x>0$ tale che $a^x \equiv 1 (m)$

esempio: l'ordine di $0(2)_7 = 3$ Cioè 3 è il minimo esponente tale che $2^3 \equiv 1 (7)$. Ma allora posso (computare l'ordine) calcolare il resto di ogni esponente

esempio 2: $2^{55} \equiv ? (7)$ $\quad 2^{55} = 2^3 \cdot 2^3 \cdots 2^1 \equiv 2 (7)$

In generale $a^x = a^{kq+r}$ con $(a,m)=1$ posso scrivere $a^x \equiv a^k \cdot a^k \cdots a^r \equiv a^r (m)$

• Teorema

Sia $(a,m)=1$ Quindi $k = o(a)_m$ esiste $a^k \equiv 1 (m)$

tesi: $a^x \equiv 1 (m) \iff o(a) \mid x$

$\iff x \equiv \emptyset (o(a)_m)$

dim ($\Leftarrow$) $a^{o(a)} \equiv 1 (m) \Rightarrow a^{o(a) \cdot l} \equiv a^{o(a)} \cdots a^{o(a)} \equiv 1 \cdot 1 \cdots 1 \equiv 1 (m)$

Cioè se x è multiplo di $\emptyset\, o(a) \Rightarrow a^x \equiv 1 (m)$

($\Rightarrow$) $a^x \equiv 1 (m) \Rightarrow x \equiv \emptyset \; (o(a)_m)$

$x = o(a) q + r \quad 0 \leq r < o(a)$

$1 \underset{ip}{\equiv} a^x \equiv a^{o(a) q + r} \equiv (a^{o(a)})^q a^r \equiv a^r \Rightarrow r = 0$

$\Rightarrow x \equiv 0 (o(a)_m)$

esempio: per quali x $\quad 3^{5x} \equiv 2 (7)$ $\iff$

$3^{5x} \equiv 3^2 (7) \iff 3^{5x-2} \equiv 1 (7) \iff 5x-2 \equiv 0 \; (o(3)_7)$

Per ottenere $o(3)_7$: $3^0 \; 3^1 \; 3^2 \; 3^3 \cdots 3^6$ dunque $o(3)_7 = 6$

$1 \quad 3 \quad 2 \quad 6 \quad 1$

-1

Dunque $5x - 2 \equiv 0 (6)$

$5x \equiv 2 (6)$

$-x \equiv 2 (6) \iff x \equiv -2 (6) \iff x \equiv 4 (6)$

• Trovare l'ordine

$o(3)_7 = 6$ per Fermat era 3^{7-1} ma il fatto che coincidano è solo un caso. Infatti $o(2)_7 = 3$ mentre per Fermat era 6. Sicuramente l'esponente di Fermat è un multiplo dell'ordine Infatti

1) Fermat $a^{p-1} \equiv 1 (p)$ $\quad p-1$ è multiplo di $o(a)_p$

2) $a^x \equiv 1 (p) \iff x$ multiplo

esempio $0 \ (7 \mid 31 \mid 31-3=30 = 3\cdot 5\cdot 2$

• Ripasso congruenze e sistemi 10/#12/13

$$\exists x \cdot \begin{cases} x \equiv a \ (m_1) \\ x \equiv b \ (m_2) \end{cases} \iff MCD(m_1, m_2) \mid a-b$$

($\Leftarrow$) Per Bezout ho che $MCD(m_1, m_2) = m_1 \mu + m_2 \nu$

$a-b = k \, MCD(m_1, m_2) = m_1(k\mu) + m_2(k\nu)$

$x \equiv a - m_1(k\mu) = b + m_2(k\nu)$

($\Rightarrow$) Se $\exists x$ che risolve il sistema $d = MCD(m_1, m_2)$

$x \equiv a \ (m_1) \Rightarrow x \equiv a \ (d)$

$x \equiv b \ (m_2) \Rightarrow x \equiv b \ (d)$ $\Rightarrow a \equiv b \ (d) \Rightarrow d \mid a-b$

Quando x esiste ne trovo una x_0. Le altre sono $x_0 + l \cdot MCM(m_1, m_2)$

• Sistemi di 3 congruenze

$$\left.\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ x \equiv a_3 \ (m_3) \end{cases}\right\} MCD(m_1, m_2) \mid a_1 - a_2 \ ?$$

NO → non c'è soluzione

SI → trovo una sol x_0 delle prime due e vado a risolvere

$$\begin{cases} x \equiv x_0 \ (MCM(m_1, m_2)) \\ x \equiv a_3 \ (m_3) \end{cases}$$

Inoltre nel caso in cui ho moduli primi tra loro vale il seguente teorema:

TEO: Se m_1, m_2, m_3 sono primi tra loro $\begin{cases} MCD(m_1, m_2) = 1 \\ MCD(m_2, m_3) = 1 \\ MCD(m_3, m_1) = 1 \end{cases}$

esiste x tale che $\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ x \equiv a_3 \ (m_3) \end{cases}$

il sistema equivale $x \equiv x_0 \ (m_1 \cdot m_2 \cdot m_3)$

esempio: $178^{561} \equiv ? \ (561)$ Se p primo $178^p \equiv 178 \ (p)$ ma 561 non è primo infatti $561 = 3 \cdot 11 \cdot 17$. Ma 561 è falso primo (è un n° di Carmichael). I falsi primi sono quei numeri non primi per i quali valgono alcune proprietà relative ai primi. In questo caso infatti $178^{561} \equiv 178 \ (561)$ perché?

$178^{561} \equiv X\ (561) \iff \begin{cases} 178^{561} \equiv X\ (3) \\ 178^{561} \equiv X\ (11) \\ 178^{561} \equiv X\ (17) \end{cases}$

Posso farlo perché
$u \equiv v\ (k) \Rightarrow u \equiv v\ (k')$ se $k' \mid k$

$u \equiv v\ (m_1) \quad m_1 \mid u - v$

$u \equiv v\ (m_2) \Rightarrow m_2 \mid u - v \Rightarrow m_1 m_2 m_3 \mid u - v \Rightarrow u \equiv v\ (m_1 m_2 m_3)$

$u \equiv v\ (m_3) \quad m_3 \mid u - v$

Per Fermat [se p primo e $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1\ (p)$]

$\begin{cases} 178^2 \equiv 1\ (3) \\ 178^{10} \equiv 1\ (11) \\ 178^{16} \equiv 1\ (17) \end{cases} \Rightarrow \begin{cases} 178^{560} \equiv 1\ (3) \\ 178^{560} \equiv 1\ (11) \\ 178^{560} \equiv 1\ (17) \end{cases}$

poiché 560 è multiplo di 2, 10, 16. Da cui moltiplicando per 178

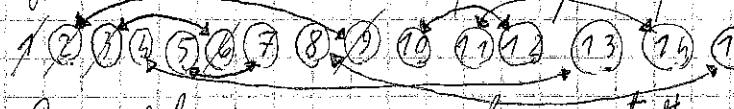
$\Leftarrow$

$\begin{cases} 178^{561} \equiv 178\ (3) \\ 178^{561} \equiv 178\ (11) \\ 178^{561} \equiv 178\ (17) \end{cases}$

È dunque per Fermat $178^{561} \equiv 178\ (3 \cdot 11 \cdot 17)$

Esempio 2 A quanto è congruo $1 \cdot 2 \cdot 3 \cdots 16 \equiv !\ (17) \iff 16! \equiv !\ (17)$

Ogni n° ha un inverso grandi passo fine diverse cancellature



Ogni n° ha un inverso perché sono tutti primi con 17

Ma per quali a: $a \cdot a \equiv 1\ (17)$! ovviamente $a = 1$, $a = 16$

dunque $a^2 \equiv 1\ (17) \Rightarrow 17 \mid (a^2 - 1) \Rightarrow 17 \mid (a+1)(a-1) \Rightarrow (17 \mid a+1) \vee (17 \mid a-1)$ (17 primo)

$\Rightarrow a \equiv -1\ (17) \vee a \equiv 1\ (17)$ Dunque abbiamo dimostrato che solo $a = 1$ e $a = 16$ moltiplicati per se stessi danno $1\ (17)$

Dunque $16! \equiv 16\ (17)$ cioè $16! \equiv -1\ (17)$

Lo stesso ragionamento mostra che se p è primo

$(p-1)! \equiv -1\ (p)$ poiché

$(p-1)! = 1 \cdot 2 \cdots (p-1)$ e $aa \equiv 1\ (p) \Rightarrow a \equiv -1\ (p)$
$a \equiv 1\ (p)$

Viene detto teorema di Wilson

1/ Es Berardinesi lezione

sia $f: \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z} = \mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \dots, \bar{9}\}$

$f(\bar{x}) = \bar{3}\bar{x}$

$f(\bar{1}) = \bar{3}$ $\quad f(\bar{2}) = \bar{6}$

è iniettiva? suriettiva?

iniettiva: $3\bar{x} = 3\bar{z} \Rightarrow x = z$ sì, è iniettiva perché

$3x \equiv 3z (10) \iff 3 \cdot 7 \cdot x = 3 \cdot 7 \cdot z (10) \iff 21x \equiv 21z (10) \iff x \equiv t (10)$

suriettiva: dato $\bar{b} \in \mathbb{Z}_{10}$ trova sempre un $\bar{a} \in \mathbb{Z}_{10}$. $f\bar{a} = \bar{b}$? $\bar{3} \cdot \bar{a} = \bar{b}$ risolvo

$3x \equiv b (10)$ esiste x infatti $x = 7b$ mai da soluzione

invertibile: Sì. Per trovarla devo avere $g(f(x)) = x$

Se $f(x) = \bar{3}x$ chi è g?

$g(y) = \bar{7}y$ in $\mathbb{Z}_{10}$

Infatti $f(g(y)) = f(7y) = 3 \cdot 7 \cdot y = 1 \cdot y = y$

Dunque è invertibile

2/ Es Berardinesi lezione

Come sopra ma $f(x) = \bar{2}x$

iniettiva: No perché $2 \cdot 1 \equiv 2 \cdot 6 \quad (10)$

$2 \equiv 2$

ma anche $2 \cdot 0 \equiv 2 \cdot 5$

suriettiva: ~~perché $\mathbb{Z}/10\mathbb{Z} = \mathbb{Z}_{10}$~~ un numero non è suriettiva. Ad esempio

$2x = 3 (10)$ non ha soluzioni poiché $MCD(10, 2) \nmid 3$

In generale

$f: \mathbb{Z}_n \to \mathbb{Z}_n \quad f(x) = ax$ è biunivoca $\iff$ esiste l'inverso di a mod $n \iff MCD(a, n) =$

3/ es Berardocci

$f: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ è iniettiva? è suriettiva? invertibile?

$f(x) = \bar{3}x + \bar{4}$

iniettiva: $3\bar{x} + 4 = 3\bar{z} + 4 \Rightarrow x = z$ SI perché $3x + 4 \equiv 3z + 4 \ (10)$ equivale a $3x \equiv 3z \ (10)$. Come in es 1 allora è iniettiva

suriettiva: SI

invertibile: $\bar{3}\bar{x} + 4 = \bar{y} \iff 3\bar{x} = y + \bar{4} = y + 6$ per "far sparire" il 3 moltiplico per 7

dunque $x = \bar{7}(y+6) \iff x = \bar{7}y + \bar{42} = \bar{7}y + \bar{2}$

quindi $g(y) = \bar{7}y + 2$ è l'inversa

11/12/13

1/ es Berardocci

$49 \mid 2^{3n+3} - 7n - 8$ equivale a $2^{3n+3} - 7n - 8 \equiv 0 \ (49)$ @ ⓐ

Si può procedere in 2 modi: 1) per induzione

2) tramite il binomio di newton

partiamo da 2) osserviamo che $2^{3n+3} = 2^{3(n+1)} = 8^{n+1} = (7+1)^{n+1}$

applichiamo adesso la formula del binomio di newton

$$\sum_{i=0}^{n+1} \binom{n+1}{i} 7^i = 1 + (n+1)7^1 + \underbrace{\binom{n+1}{2} 7^2 + \dots}_{\equiv 0 \bmod 49} \equiv 1 + (n+1)7$$

sostituendo in ⓐ si ottiene:

$1 + (n+1)7 \equiv 7n + 8 \ (49)$

$7n + 8 \equiv 7n + 8 \ (49)$

1) Facciamolo adesso per induzione.

Caso base: per $n = 0$ $2^{3 \cdot 0 + 3} \equiv 8 \ (49)$ è vera

Caso induttivo: supponendolo vero per n, cerchiamo di verificarlo per $n+1$

$2^{3(n+1)+3} \equiv 7(n+1) + 8 \ (49) \iff 2^{3n+3} \cdot 8 \equiv 7(n+1) + 8 \ (49)$ per ipotesi induttiva

$(7n+8) \cdot 8 \equiv 7(n+1) + 8 \ (49)$ per finire basta dimostrare la congruenza $56n + 64 \equiv 7(n) + 7 + 8 \ (49) \iff 7n + 15 \equiv 7n + 15 \ (49)$

che è vera.

2 / es Berardinucci

$a_0 = 1, \quad a_1 = 4, \quad \underbrace{a_{n+2} = \frac{a_{n+1} + a_n}{2}}_{(*)} = \frac{1}{2} a_{n+1} + \frac{1}{2} a_n$

trovare una formula esplicita

È necessario che si cerchi di risolvere (*) senza preoccuparsi inizialmente delle condizioni iniziali.

Poniamo con $a_n = x^n$. Sostituiamo in (*)

$x^{n+2} = \frac{1}{2} x^{n+1} + \frac{1}{2} x^n$ divido per x^n: $x^2 = \frac{1}{2} x + \frac{1}{2}$ risolviamo ottenendo $x = 1$ e $x = -\frac{1}{2}$. Entrambi verificano (*). Però nessuno dei due verifica le condizioni iniziali. Ne prendo allora una combinazione lineare

$$\begin{cases} a_n = A \cdot 1^n + B \cdot \left(-\frac{1}{2}\right)^n \\ 1 = A \cdot 1^0 + B \cdot \left(-\frac{1}{2}\right)^0 = A + B \\ 4 = A \cdot 1^1 + B \cdot \left(-\frac{1}{2}\right)^1 = A - \frac{1}{2} B \end{cases} \quad \begin{cases} A = 3 \\ B = -2 \end{cases}$$

Quindi la soluzione è

$a_n = 3 + (-2)\left(-\frac{1}{2}\right)^n$

Controllo la (*): cioè posso scrivere $a_{n+2} - \frac{1}{2} a_{n+1} - \frac{1}{2} a_n = 0$ con $a_n = A \cdot 1^n + B \cdot \left(-\frac{1}{2}\right)^n$ dunque:

$$A + B \cdot \left(-\frac{1}{2}\right)^{n+2} - \frac{1}{2}\left[A + B\left(-\frac{1}{2}\right)^{n+1}\right] - \frac{1}{2}\left[A + B\left(-\frac{1}{2}\right)^n\right] =$$

$$= B \cdot \left[\left(-\frac{1}{2}\right)^{n+2} - \frac{1}{2}\left(-\frac{1}{2}\right)^{n+1} - \frac{1}{2}\left(-\frac{1}{2}\right)^n\right] = B\left(-\frac{1}{2}\right)^n \left[\left(-\frac{1}{2}\right)^2 - \frac{1}{2}\left(-\frac{1}{2}\right)^1 - \frac{1}{2}\left(-\frac{1}{2}\right)^0\right] = 0$$

Più in generale se ho

$a_{n+3} = c_1 a_{n+2} + c_2 a_{n+1} + c_3 a_n$ devo scriverlo come

(*') $a_{n+3} - c_1 a_{n+2} - c_2 a_{n+1} - c_3 a_n = 0$ ponendo $a_n = x^n$, $a_{n+1} = x^{n+1}$ ... e semplifico

$x^3 - c_1 x^2 - c_2 x - c_3 = 0$ (polinomio caratteristico)

Trovate le soluzioni del polinomio, verificheranno (*'). Se una delle radici rispetta le condizioni iniziali allora ho concluso. Ma se così non fosse, dette x_0, x_1, x_2 le soluzioni del nostro polinomio avrò che

$a_n = A x_0^n + B x_1^n + C x_2^n$ che sicuramente rispetta (*'). Ma avendo io le 3 condizioni iniziali (nel nostro esempio) allora potrò risolvere il sistema a fianco, trovare $A, \ldots$

$$\begin{cases} a_0 = A x_0^0 + B x_1^0 + C x_2^0 \\ a_1 = A x_0^1 + B x_1^1 + C x_2^1 \\ a_2 = A x_0^2 + B x_1^2 + C x_2^2 \end{cases}$$

Supponendo che il nostro polinomio sia: $x^3-6x^2-12x-6$ svolgiamo il seguente esercizio:

Sia $a_{n+3}=6a_{n+2}+12a_{n+1}+6a_n$ (*'') $a_0=1$ $a_1=0$ $a_2=2$

Il nostro pol. caratt. è quello sopra, $a_n=1^n, 2^n, 3^n$ potrebbero risolvere (*'') includendo anche le condizioni iniziali. Ognuna $a_n=A1^n+B2^n+C3^n$ che sicuramente risolve (*''). Determiniamo allora A, B, C dalle 3 condizioni iniziali

$$\begin{cases} a_0=1=A\cdot 1^0+B\cdot 2^0+C\cdot 3^0 \\ a_1=0=A\cdot 1^1+B\cdot 2^1+C\cdot 3^1 \\ a_2=2=A\cdot 1^2+B\cdot 2^2+C\cdot 3^2 \end{cases}$$

Vediamo invece quando è che il metodo suddetto non funziona

(*''') $a_{n+2}=4a_{n+1}-4a_n$ lo riscrivo come $a_{n+2}-4a_{n+1}+4a_n=0$ $\begin{cases} a_0=5 \\ a_1=7 \end{cases}$

$p(x)=x^2-4x+4=(x-2)(x-2)=(x-2)^2=0$

$a_n=2^n$ è soluzione di (*''') ma non ho abbastanza condizioni per risolvere In caso di soluzioni doppie possiamo sicuramente dire che anche $a_n=n\cdot 2^n$ è soluzione di (*'''). Allora posso scrivere:

$a_n=A\cdot 2^n+Bn\cdot 2^n$. Risolviamo allora il sistema:

$$\begin{cases} a_0=5=A\cdot 2^0+B\cdot 0\cdot 2^0 \\ a_1=7=A\cdot 2^1+B\cdot 1\cdot 2^1 \end{cases} \quad \begin{cases} 5=A \\ -\frac{3}{2}=B \end{cases}$$

Dunque la soluzione che rispetta le condizioni iniziali e (*''') è:

$a_n=5\cdot 2^n+\left(-\frac{3}{2}\right)n\cdot 2^n$

17/12/13

1/ Lezione Bernducci

$5^{5x} \equiv 4 (21) \iff 5^{5x} \equiv 4 (3) \iff \begin{cases} 2^{5x} \equiv 1 (3) \\ 5^{5x} \equiv 4 (7) \end{cases} \quad \begin{cases} 2^{5x} \equiv 1 (3) \\ 5^{5x-2} \equiv 1 (7) \end{cases}$

~~$\iff 5x \equiv 0 \pmod 6$~~ Per Fermat $5^6 \equiv 1 (7)$ ma devo cercare tra i divisori se ne esiste uno più piccolo che ripete $5^m \equiv 1 (7)$

$5^2 \equiv 4 (7)$ Dunque 6 è la soluzione

$5^3 \equiv -1 (7)$

$5^6 \equiv 1 (7)$

Allora devo risolvere $\begin{cases} x \equiv 0 (2) \\ x \equiv 4 (6) \end{cases}$ dunque $x = 4 + 6k$

2/ Lezione Bernducci

$13^x \equiv 1 (23)$ $x = 22$ è ovviamente soluzione è da verificare se i suoi divisori sono soluzioni

3/ Lezione Bernducci

Quante sono le coppie (A, B) con $A \subseteq B \subseteq \mathbb{N}_{10}$ * (con A, B insieme)

Gli $A \subseteq \mathbb{N}_{10}$ sono 2^{10} Li fa in 3 modi

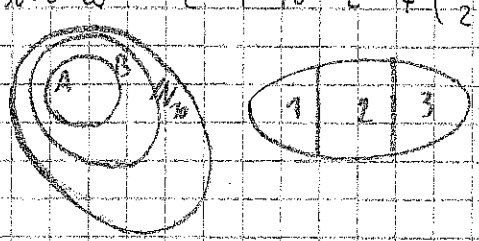
(a) per casi $|A| = 0$ ho 2^{10} scelte per B

$|A| = 1$ ho 2^9 scelte per B

$\vdots$

$|A| = 10$ ho 2^0 scelte per B

In totale $2^{10} + 10 \cdot 2^9 + \binom{10}{2} \cdot 2^8 + \dots + \binom{10}{10} \cdot 2^{10} = \sum_{i=0}^{10} \binom{10}{i} 2^{10-i} = (2+1)^{10} = 3^{10}$

(b) 

$g: \mathbb{N}_{10} \to \mathbb{N}_3$ associo a g la coppia (A, B) con $A = \{x \in \mathbb{N}_{10} \mid g(x) = 1\}$

4/ Lezione Bernducci

Quante sono le $f: \mathbb{N}_{20} \to \mathbb{N}_{30}$ tali che $\mathrm{Im}(f)$ contiene almeno 2 pari

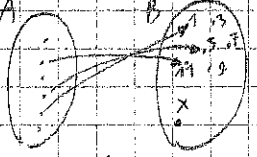
Per complemento: TUTTE - (nessun pari + 1 solo pari)

TUTTE: 30^{20}

nessun pari: sono 15^{20} (ho 15 scelte, cioè tutti i dispari)

1 solo pari: sono $15 \cdot (16^{20} - 15^{20})$

- 15: modi di scegliere il solo pari
- $(16^{20} - 15^{20})$: modi in cui scelgo i 15 dispari più il pari. Sono cioè le funzioni che vanno da:



dove x è il pari che ho scelto

← Sono tutte le funzioni che dal dominio vanno solo nei dispari. Dunque sottraendo quelle che vanno solo nei dispari ottengo le funzioni che hanno uno solo pari e un solo pari.

Ma queste (16^{20}) sono quelle che hanno AL MASSIMO un elemento x pari nell'Imm(f)

Dunque $30^{20} - (15^{20} + 15(16^{20} - 15^{20}))$

5/ Les. Bernducci

$50^{4226} \equiv ? \ (23) \iff 4^{4226}$ per Fermat $4^{22} \equiv 1 \ (23)$

Ma allora sapendo che $4226 \mid 22$, $202 \mid 102$ Ma allora $4^{4224} \equiv 1 \ (23)$

E dunque $4^{4226} = 4^{4224} \cdot 4^{22} \equiv ? \ (23)$ Dunque $4^2 \equiv ? \ (23)$ cioè 16

$50^{4226} \equiv 16 \ (23)$

6/ Les Bernducci

$4^x \equiv 1 \ (7)$ per Fermat $4^6 \equiv 1 \ (7)$ Ciecamente se $x = 6 \cdot k$ (multiplo di 6)

x risolve ma ad esempio $4^2 \equiv 2 \ (7)$ E quindi $x = 3 \cdot k$ cioè basta che

$4^3 \equiv 1 \ (7)$ x sia multiplo di 3

7/ es Berardocci

Di quanto è congruo in mod 5 l'n-esimo n° di Fibonacci?

$f_n \equiv ? \ (5)$

1 1 2 3 5 8 13 21 34

1 1 2 3 0 3 3 1 4 0 4 4 3 2 0 2 2 4 1 0 1 1 2 3

periodo ogni 20

8/ es Berardocci

$a_0 = 3 \quad a_1 = -2 \quad a_n = a_{n-1} + 12 a_{n-2} \iff x^2 - x - 12 = 0$ troviamo le radici

$(x-4)(x+3) = 0$ ok nella forma 4^n e -3^n, Nessuno dei 2 rispetta le condizioni iniziali dunque ne cerco una comb. lineare

$a_n = A \cdot 4^n + B(-3)^n$

$$\begin{cases} 3 = A + B \\ -2 = A \cdot 4 + B \cdot (-3) \end{cases} \quad \begin{cases} A = 1 \\ B = 2 \end{cases}$$