Esercitazioni di Matematica Discreta

C.S. in Informatica

Università di Genova

Lucidi delle esercitazioni
e
Fogli di esercizi
con suggerimento o risposta

Genova, 24 dicembre 2007

Rosalba Barattero
Dipartimento di Matematica
http://www.dima.unige.it/~baratter
DIMA

Parte I

Lucidi delle Esercitazioni

ESERCITAZIONE N.1

9 ottobre 2007

- I numeri naturali
- Il principio di induzione
- Primi esempi sulle funzioni

Rosalba Barattero

I NUMERI NATURALI

L'insieme dei numeri naturali è l'insieme infinito

$\mathbb{N} = \{0,1,2,3,...\}$ la cui prima funzione è 'contare'.

Conosciamo le operazioni di $\mathbb{N}$:

- l'addizione,
- la moltiplicazione,
- la divisione con il resto (la vedremo in dettaglio nel corso),
- la potenza con esponente ≥ 0

  $a^0 = 1$, $a^n = a \cdot a \cdot a \cdot ... \cdot a$ (n volte)

• la sottrazione non è operazione in $\mathbb{N}$ poiché il risultato può essere un numero negativo $n \notin \mathbb{N}$

Sappiamo usare anche le proprietà di $\mathbb{N}$ e delle sue operazioni : commutativa della somma, associativa, ...

E sappiamo confrontare due numeri distinti di $\mathbb{N}$, cioè dati $a, b \in \mathbb{N}$ sappiamo stabilire se $a<b$ oppure $a>b$.

Ma matematicamente porre $\mathbb{N} = \{0,1,2,3,...\}$ non vuol dire averlo definito, poiché è un insieme infinito !

Il modo corretto è di dare una definizione che caratterizzi tutti i suoi elementi. Si procede così dando gli ASSIOMI e deducendo poi da essi altre proprietà vere in $\mathbb{N}$.

Ogni numero n, ha un successore, indicato con s(n), e iterando il successore non si ottiene mai un numero già considerato, perché i successori di due numeri diversi sono diversi.

Questi sono i primi 4 **ASSIOMI DI PEANO**

A1: *Esiste un numero naturale* 0.
A2: *Ogni numero naturale* a *ha un successore denotato* $S(a)$.
A3: 0 *non è il successore di alcun numero naturale.*
A4: *Numeri naturali distinti hanno successori distinti.*

Inoltre in $\mathbb{N}$ ogni suo elemento si ottiene da 0 iterando un numero finito di volte l'operazione di successore. Interviene così l'ultimo assioma, **5° ASSIOMA DI PEANO A5, detto principio di induzione:**

PRINCIPIO DI INDUZIONE

Data una proprietà, se è tale che :

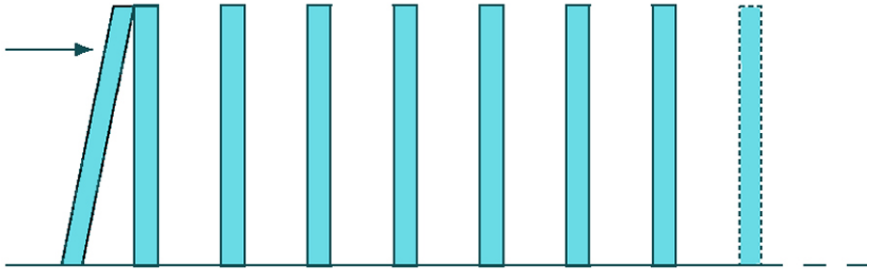
(a) la proprietà vale per 0

(b) ogni volta che la proprietà vale per un generico numero naturale allora vale anche per il suo successore,

allora la proprietà vale per tutti i numeri naturali.

Un'immagine comoda per rappresentarsi la situazione è quella di una successione di pezzi di domino messi in piedi in equilibrio precario , distanti tra loro meno della loro altezza.

Così se un pezzo cade verso destra fa cadere verso destra quello adiacente. Se cade il primo, fa cadere il secondo, che fa cadere il terzo,e tutti cadono.



[da G. Lolli – Logica Matematica – Corso di laurea in Informatica 2005-2006]

Non fa parte del nostro programma studiare la costruzione di $\mathbb{N}$ a partire dai 5 assiomi di Peano, ci interessa invece il

Principio di induzione, come regola per dimostrare proprietà che sono vere per tutti i numeri naturali o più precisamente a partire da un numero naturale in avanti .

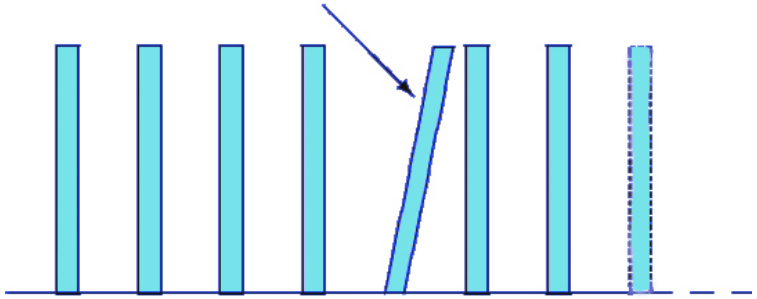
Il principio di induzione può essere schematizzato così, indicando con P(n) la proposizione espressa per il numero naturale n

- BASE : $P(0)$
- PASSO INDUTTIVO: $\forall\, n \geq 0$ si ha $P(n) \Rightarrow P(n+1)$

$\forall\, n\ P(n)$

Precisazione. La base non si riferisce necessariamente al numero zero, ma al 'primo' numero per cui la proprietà ha significato.

Se ad esempio il primo pezzo a cadere è il quinto, cadono allora tutti i pezzi dal quinto in poi



Quindi riformuliamo il Principio di induzione:

PRINCIPIO DI INDUZIONE GENERALIZZATO

Data una proprietà, se è tale che :

(a) la proprietà vale per $k \in \mathbb{N}$

(b) ogni volta che la proprietà vale per un generico numero naturale $n \geq k$ allora vale anche per il suo successore $n+1$,

allora la proprietà vale per tutti i numeri naturali $n \geq k$.

Vediamo il primo esempio:

ESERCIZIO 1.

Il principio di induzione:la somma dei primi n numeri naturali

Provare per induzione che vale la seguente proprietà per ogni numero naturale $n \geq 1$

(*) $1+2+3+\ldots+n = \frac{n(n+1)}{2}$.

Per provare che (*) è vera **per ogni n≥1** usiamo il principio di induzione.

BASE DELL'INDUZIONE: La proprietà è *vera per n=1*.

In (*) $1+2+3+\ldots+n = \frac{n(n+1)}{2}$,

sostituiamo n=1 e otteniamo: $1 = \frac{1(1+1)}{2}$, vero.

PASSO DELL'INDUZIONE: Se la proprietà (*) è vera per un generico n≥1 allora è vera anche per il successivo n+1

Supponiamo di sapere che la proprietà valga per n, n≥1

$1+2+3+\ldots+n = \frac{n(n+1)}{2}$ ← **IPOTESI** INDUTTIVA.

Mostriamo che la proprietà vale per n+1 ← TESI

Come si esprime la tesi ?

Sostituiamo n+1 al posto di n in $1+2+3+\ldots+ n= \frac{n(n+1)}{2}$.

$1+2+3+\ldots+ (\mathbf{n+1})= \frac{(n+1)((n+1)+1)}{2}$,cioè

$1+2+3+\ldots+ (n+1) = \frac{(n+1)(n+2)}{2}$. ← **TESI**

Ora si tratta di dedurre dall'ipotesi $1+2+3+\ldots+n= \frac{n(n+1)}{2}$

la tesi $1+2+3+\ldots + (n+1) = \frac{(n+1)(n+2)}{2}$, tramite calcolo.

Scriviamo il membro di sinistra dell'uguaglianza della tesi:

$$\underbrace{1+2+3+\ldots+n}+(n+1) =$$

Uguali per l'ipotesi induttiva

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

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

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

Allora la tesi è vera !

CONCLUSIONE: per il principio di induzione la proprietà (*) è vera per tutti i numeri naturali $n \geq 1$.

OSSERVAZIONE .

Il principio di induzione serve per provare la verità di un asserto già noto per altre vie, anche se talvolta può suggerirne la risposta.

Come si è arrivati alla formula $1+2+3+\ldots+ n = \frac{n(n+1)}{2}$?

Gauss, uno dei più grandi matematici, nel 1787, all'età di 10 anni calcolò mentalmente **la somma dei numeri da 1 a 100**, rispondendo ad un compito assegnato dal maestro.

Come fece Gauss ?

Li sommò a coppie in questo ordine :

1+100 = 101
2+99 = 101
3+98 = 101
...
50+51 = 101

La somma di queste 50 coppie di numeri è 50·101=**5050**.

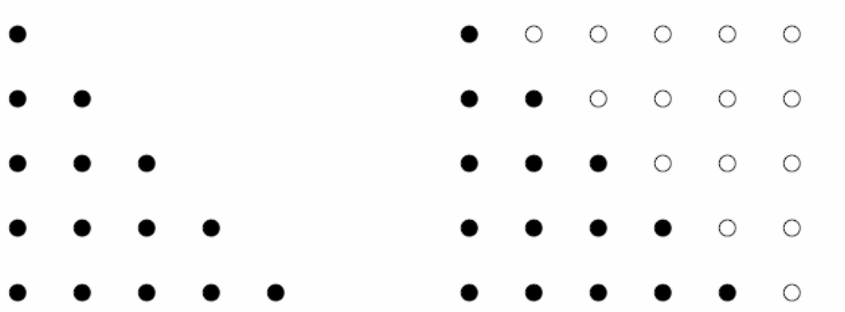
In generale per **sommare i numeri da 1 ad n**, scriviamo 2 volte la somma , ordinando gli addendi in modo crescente e decrescente

$$\begin{array}{ccccccccccc} 1 & + & 2 & + & \dots & + & (n-2) & + & (n-1) & + & n \\ n & + & (n-1) & + & \dots & + & 3 & + & 2 & + & 1 \\ \hline (n+1) & + & (n+1) & + & \dots & + & (n+1) & + & (n+1) & + & (n+1) \end{array}$$

In ogni riga ci sono n addendi quindi la somma finale vale n(n+1) ed è il doppio della somma cercata, da cui

$$1+2+3+\dots+n = \frac{n(n+1)}{2}.$$

Un ulteriore modo 'geometrico' è il seguente:



1+2+3+4+5=?

2(1+2+3+4+5)= 5·6=30

ESERCIZIO 2.

Il principio di induzione – esempio geometrico

Provare per induzione che la somma degli angoli interni di un poligono convesso con n lati è π (n - 2).

La proprietà ha senso a partire dal triangolo (n=3).

Quindi in questo caso il principio di induzione correttamente enunciato è :

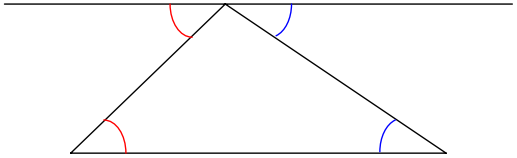
- BASE : P(3)
- PASSO INDUTTIVO: $\forall$ n $\geq$ 3 si ha P(n) $\Rightarrow$ P(n+1)

$\forall$ n P(n)

In parole:

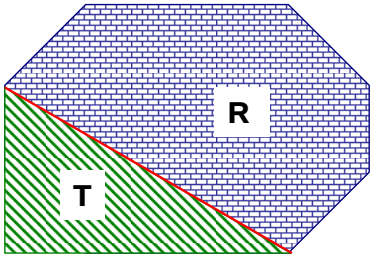
detta P(n) la proposizione "la somma degli angoli interni di un poligono convesso con n lati è π (n - 2)", per provare che è vera $\forall$ n sono sufficienti *due mosse*:

- la prima consiste nel dimostrare che è *vera per n=3*
- la seconda nel dimostrare che *se è vera per un generico* n (n ≥3) allora *è vera anche per il successivo* n+1.



BASE

P(3): somma angoli interni è $\pi=\pi(3-2)$



PASSO INDUTTIVO

Il poligono dato, che nella figura immaginiamo avere n lati, si suddivide nel poligono R avente n-1 lati e nel triangolo T.

Per *I' ipotesi induttiva* si sa che la somma degli angoli interni di R è $\pi((n-1)-2)$.

A questo punto basta aggiungere la somma degli angoli interni di T, che vale π, per ottenere la somma degli angoli interni del poligono dato :

$$\pi((n-1)-2)+\pi=\pi(n-2) \qquad \text{ok!}$$

ESERCIZIO 3.

Il principio di induzione:la somma dei dispari

Provare per induzione che vale la seguente proprietà per ogni numero naturale $n \geq 1$

(*) $1+3+5+\ldots+(2n-1)=n^2$.

(pari = multiplo di 2 = 2n, dispari= successivo o antecedente di un pari = 2n+1 opp. 2n-1)

E' la *somma* dei primi n *numeri naturali dispari* consecutivi.

$$1 = 1 = 1^2$$
$$1+3 = 4 = 2^2$$
$$1+3+5 = 9 = 3^2$$
$$1+3+5+7 = 16 = 4^2$$

.....

Per provare che (*) è vera **per ogni n≥1** usiamo il principio di induzione.

BASE DELL'INDUZIONE: La proprietà è *vera per n=1*.

Sostituiamo n=1 in (*), otteniamo: $1 = 1^2$, vero (v.sopra).

PASSO DELL'INDUZIONE: Se la proprietà (*) è vera per un generico n≥1 allora è vera anche per il successivo n+1.

Supponiamo di sapere che la proprietà valga per n, n≥1

$1+3+5+\ldots+(2n-1)=n^2$ ← **IPOTESI** INDUTTIVA.

Mostriamo che la proprietà vale per n+1 ← TESI

Come si esprime la tesi ?

Sostituiamo in (*) n+1 al posto di n

$1+3+5+\ldots+(2(\mathbf{n+1})-1)=(\mathbf{n+1})^2$,cioè

$1+3+5+\ldots+(2n+1)=(n+1)^2$. ← **TESI**

Ora si tratta di dedurre dall'ipotesi $1+3+5+\ldots+(2n-1)=n^2$

la tesi $1+3+5+\ldots+(2n+1)=(n+1)^2$, tramite calcolo.

l'addendo immediatamente precedente
è 2n-1 (il numero dispari che precede)

$$\underbrace{1+3+5+\ldots(2n-1)}_{=n^2 \text{ per ipotesi}}+(2n+1)=n^2+(2n+1)=(n+1)^2$$

Allora la tesi è vera.

CONCLUSIONE: per il principio di induzione la proprietà (*)

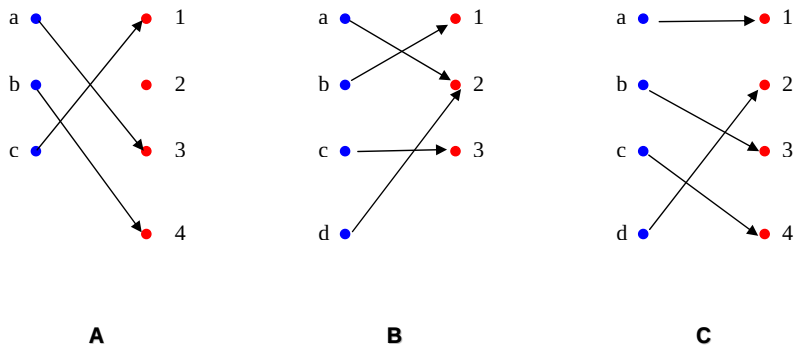
è vera per tutti i numeri naturali n≥ 1.

In simboli (*) si scrive così :

$$\sum_{n=1}^{k}(2n-1)=k^2$$

ESERCIZIO 4.

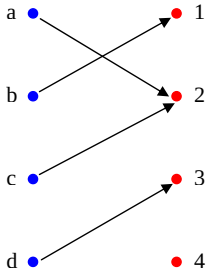
Quali sono funzioni e quali sono iniettive, surgettive ?



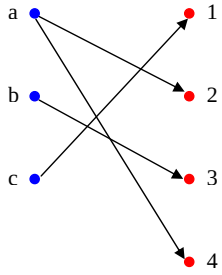
A

B

C



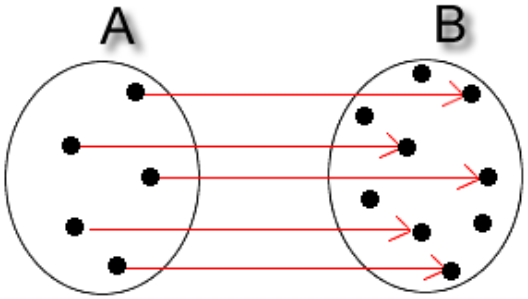
D



E

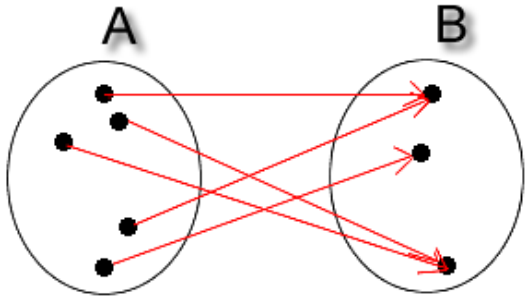
- f è una **funzione** se ad ogni elemento dell'insieme di partenza (**dominio**) fa corrispondere uno ed un solo elemento dell'insieme di arrivo (**codominio**) .

- f è *iniettiva* se trasforma elementi distinti del dominio in elementi distinti del codominio



″ f è iniettiva se i bersagli che vengono raggiunti, lo sono con una sola freccia ! ″

- f:A → B è **surgettiva** se Im(f) = {f(x)| x∈A } (Immagine di f) coincide con B. Ciò vuol dire che ogni elemento di B proviene da almeno un elemento di A : ∀ b∈B ∃ a ∈ A t.c. f(a)=b



"f è surgettiva se tutti i bersagli vengono raggiunti."

RISPOSTE

A: funzione iniettiva , non surgettiva
B: funzione surgettiva, non iniettiva
C: funzione iniettiva, surgettiva
D: funzione né iniettiva, né surgettiva
E: non è funzione

ESERCITAZIONE N.2

16 ottobre 2007

- Funzioni
- Iniettività , surgettività
- Immagine, Controimmagine
- Invertibilità di funzioni

Rosalba Barattero

GLI INSIEMI NUMERICI

$\mathbb{N} = \{0,1,2,3,4,\ldots,\ldots\}$ I NUMERI NATURALI

$Z = \{\ldots -3,-2,-1,0,1,2,3,\ldots\}$ GLI INTERI

$Q = \{\frac{m}{n} \mid m, n \in Z \text{ e } n \neq 0\}$ I RAZIONALI

$R = Q \cup \{\text{irrazionali}\}$ I REALI

$$\mathbb{N} \subset Z \subset Q \subset R$$

Chi sono gli irrazionali ?

Se passiamo alla rappresentazione decimale abbiamo ad esempio

$\frac{1}{2} = 0{,}5$

$\frac{1}{3} = 0{,}333333\ldots = 0{,}\overline{3}$

$\frac{1}{7} = 0{,}142857142857\ldots = 0{,}\overline{142857}$

$\frac{1}{109} = 0.009174311926605504587155963302752293577981651376146788990825688073394495412844036697247706422018348623853211009174\ldots\ldots\ldots$

(il periodo è di 108 cifre !)

- I razionali sono i decimali limitati (interi o con un n° finito di cifre significative dopo la virgola) e i decimali illimitati periodici.
- Gli irrazionali come ad esempio $\sqrt{2}$, π, e, ... sono decimali illimitati e **non** periodici.

ESERCIZIO 1.

Riconoscere le funzioni iniettive, surgettive

Delle seguenti funzioni stabilire se sono iniettive, surgettive :

a) f: $Z \to Z$ definita da $f(x)=2x$

b) f: $Q \to Q$ definita da $f(x)=2x$

c) f:$Q \to Q$ definita da $f(x)=x^2$

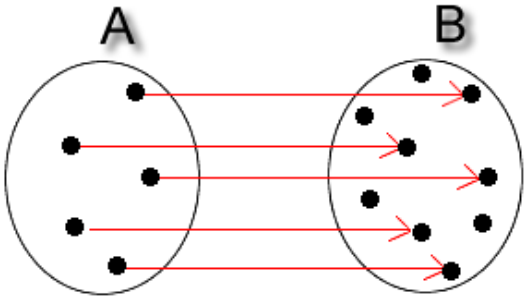
d) f:$R \to R$ definita da $f(x) = \sqrt{|x|}$

e) f:$R \to R$ definita da $f(x) = x^3$

f) f:$R \to R$ definita da $f(x) = x^3-x$

Ricordiamo che :

- f è *iniettiva* se trasforma elementi distinti del dominio in elementi distinti del codominio

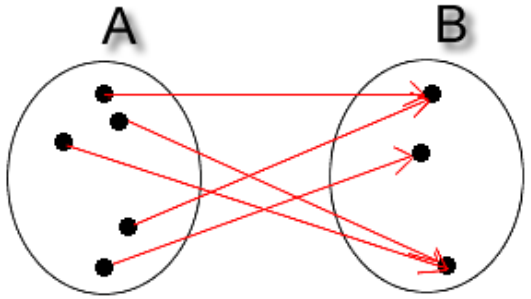


″ f è iniettiva se i bersagli che vengono raggiunti, lo sono con una sola freccia ! ″

- f:$A \to B$ è **surgettiva** se

  $Im(f) = \{f(x) \mid x \in A\}$ (Immagine di f) coincide con B.

  Ciò vuol dire che ogni elemento di B proviene da almeno un elemento di A : $\forall\, b \in B\ \exists\, a \in A$ t.c. $f(a)=b$



"f è surgettiva se tutti i bersagli vengono raggiunti."

a) f: $Z \to Z$ definita da $f(x)=2x$

Non è surgettiva: $Im(f) = \{$interi pari$\}$, ad es. $1 \notin Im(f)$

E' iniettiva : $f(x)=f(y) \Rightarrow x=y$ per ogni $x, y \in Z$

$f(x) = 2x$, $f(y) = 2y \Rightarrow 2x=2y \Rightarrow x=y$ OK!

b) f: $Q \to Q$ definita da $f(x)=2x$

E' iniettiva (come a))

E' surgettiva ? Per ogni $y \in Q$ (codominio) $\exists\, x \in Q$ (dominio) t.c. $f(x)=y$, cioè $2x=y$? sì $x=\frac{y}{2}$ $(\in Q)$

c) f:Q→Q definita da $f(x)=x^2$

Non è iniettiva : $1 \neq -1$, ma $f(1)=f(-1)=1$

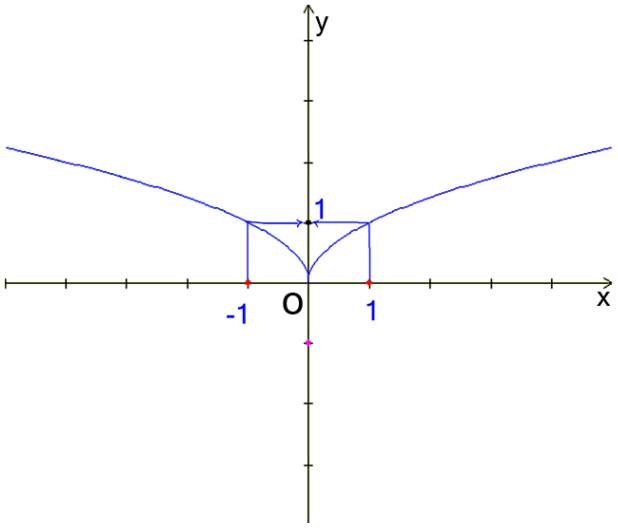
Non è surgettiva : $Im(f)=\{$razionali $\geq 0\}$ o più semplicemente : $-1 \in Q$, ma non esiste $x \in Q$ t.c. $x^2=-1$

d) f:R→R definita da $f(x) = \sqrt{|x|}$

Non è iniettiva : $1 \neq -1$, ma $f(1)=f(-1)=1$

Non è surgettiva : $-1 \in R$, ma non esiste $x \in R$ t.c. $\sqrt{|x|}=-1$

Osserviamo che questa è una funzione dell'analisi reale e come tale possiamo tracciarne il grafico e visualizzare le ns. informazioni

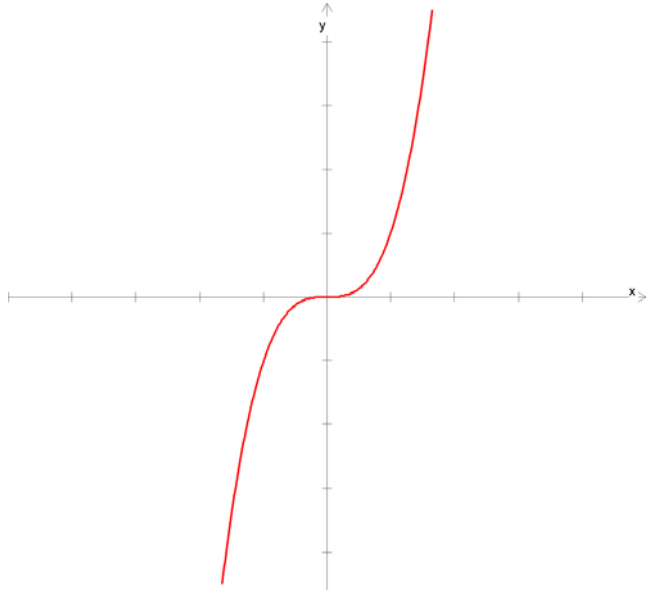


f non è né iniettiva , né surgettiva

e) f:R→R definita da $f(x) = x^3$

- f iniettiva: $f(x)=f(y) \Rightarrow x^3=y^3 \Rightarrow x=y$
- f surgettiva : $\forall\, y \in$ R (codominio) $\exists\, x \in$ R (dominio) t.c. $f(x)= y$, ossia $x^3=y$?

  Sì, supposto noto y, si ricava $x=\sqrt[3]{y}$, $x \in$ R.



f è sia iniettiva che surgettiva

f) $f:R\to R$ definita da $f(x) = x^3-x$

- f NON è iniettiva: $0\neq 1$, e $f(0)=f(1)=0$

  (il grafico ce ne dà l'interpretazione analitica)

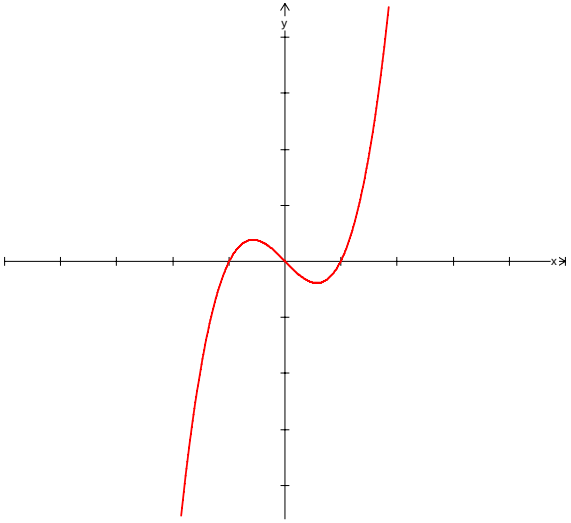
- f è surgettiva: occorre provare che

  $\forall\, y\in$ R (codominio) $\exists\, x\in$ R (dominio) t.c.

  $f(x)= y$, ossia $x^3-x =y$

  Con gli strumenti algebrici di cui disponiamo ora, non ci è possibile stabilire se l'equazione nell'incognita x (y è considerato termine noto) ha almeno una soluzione reale.

  La risposta tramite il grafico :



f non è iniettiva, è surgettiva

ESERCIZIO 2.

Controimmagini – iniettività - surgettività

Sia $f : \mathbb{N} \times \mathbb{N} \to Z$ la relazione così definita $f(m,n) = m+n$.

a) Verificare che f è una funzione.

b) Determinare f(0,1), f(1,0), f(2,3) (= immagini di elementi di $\mathbb{N} \times \mathbb{N}$).

c) Determinare $f^{-1}(0)$ (= controimmagine di $0\in Z$ tramite f), $f^{-1}(1)$, $f^{-1}(-2)$.

d) Stabilire se f è iniettiva, surgettiva.

- $\mathbb{N} \times \mathbb{N}$: prodotto cartesiano di due insiemi

  Il **prodotto cartesiano** A x B di due insiemi A e B è per def. l'insieme di tutte le coppie ordinate (a,b) con $a\in$ A e $b\in$ B.

- f è una **funzione** se ad ogni elemento dell'insieme di partenza (**dominio**) fa corrispondere uno ed un solo elemento dell'insieme di arrivo (**codominio**) .

  A ogni $(m,n)\in \mathbb{N}\times\mathbb{N}$ la nostra f fa corrispondere m+n, $m+n \in \mathbb{N} \subseteq Z$ e il valore della somma m+n è unico.

b) $f : \mathbb{N} \times \mathbb{N} \to Z$ definita da $f(m,n) = m+n$.

Determinare $f(0,1)$, $f(1,0)$, $f(2,3)$

$f(0,1) = ?$ $\quad f: \mathbb{N}\times\mathbb{N} \to Z$

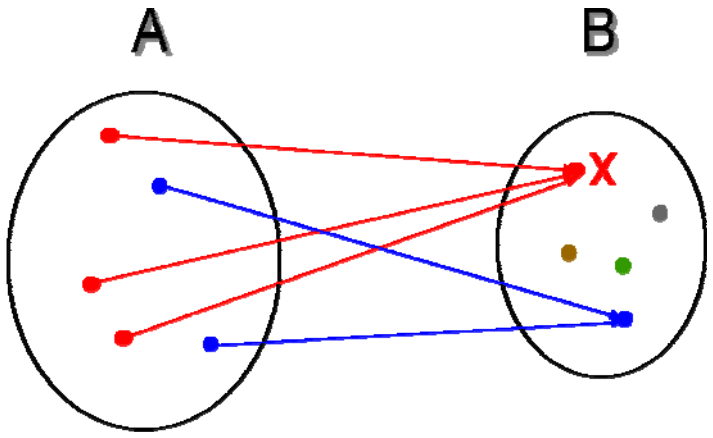
$(0,1) \to 0+1 = 1 \Rightarrow f(0,1) = 1$

$f(1,0) = 1+0 = 1 \Rightarrow f(1,0) = 1$

$f(2,3) = 2+3 = 5 \Rightarrow f(2,3) = 5$

c) Determinare $f^{-1}(0)$ (=controimmagine di 0 tramite f),

$f^{-1}(1)$, $f^{-1}(-2)$.



$f: A \to B$, $x \in B$: $f^{-1}(x) = \{a \in A \mid f(a) = x\}$

c) $f^{-1}(0) = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid f(m,n) = 0\}$

$= \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m+n = 0\}$

$= \{(0,0)\}$

$f^{-1}(1) = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid f(m,n) = 1\}$

$= \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m+n = 1\}$

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

$f^{-1}(-2) = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m+n = -2\} = \varnothing$

d) f è **iniettiva** se e solo se :

$x \neq y$ in A $\Rightarrow$ $f(x) \neq f(y)$ in B

o equivalentemente

$f(x) = f(y)$ in B $\Rightarrow x = y$ in A

f **non** è **iniettiva** perché da b) sappiamo che (0,1) e (1,0) sono due elementi distinti di $\mathbb{N} \times \mathbb{N}$ che hanno uguale immagine mediante f : $f(0,1)=f(1,0)= 1$

- Possiamo anche fare uso del concetto di controimmagine per caratterizzare l'iniettività:

$f:A \to B$ è **iniettiva** $\Leftrightarrow \forall\, b \in B$ risulta : $f^{-1}(b) = \varnothing$ oppure $f^{-1}(b) = \{a\}$, $a \in A$

da c) sappiamo che $f^{-1}(1) = \{(0,1),(1,0)\} \Rightarrow$ f non iniettiva

f: $\mathbb{N}x\,\mathbb{N} \to Z$ così definita f (m,n) = m+n

f è **surgettiva** se per ogni $x \in Z$ esiste $(m,n) \in \mathbb{N}x\mathbb{N}$

t.c. m+n = x.

Ciò è falso: se x=-2 non esistono m ed n naturali t.c. m+n = -2. Quindi la nostra f NON è surgettiva.

- Oppure possiamo anche fare uso del concetto di controimmagine per caratterizzare la surgettività:

f:A $\to$B è **surgettiva** $\Leftrightarrow \forall b \in$ B risulta $f^{-1}(b) \neq \varnothing$

ossia equivalentemente:

f:A $\to$B **non è surgettiva** $\Leftrightarrow \exists\, b \in$ B t.c. $f^{-1}(b) = \varnothing$

Dunque poiché abbiamo trovato un elemento –2 del co-dominio la cui controimmagine $\mathbf{f^{-1}(-2)}$ è vuota, ne consegue che f Non è surgettiva

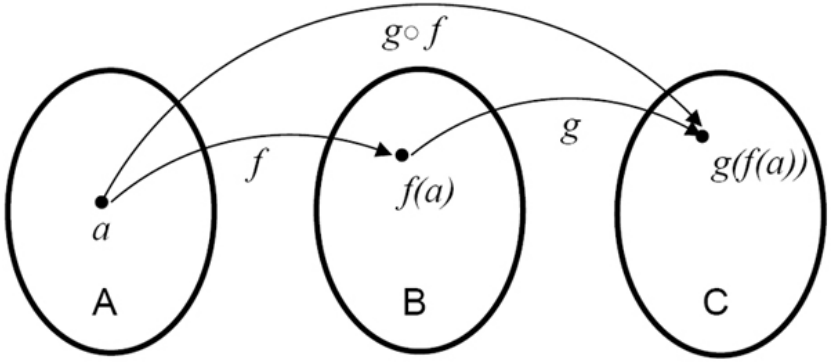
ESERCIZIO 3.

E' la funzione inversa ?

Sia f: ZxZ $\to$ ZxZ la funzione definita da f(x,y) = (x-y+1, x+1). Provare che g: ZxZ $\to$ ZxZ definita da g(a,b) = (b-1,b-a) è l'inversa di f.

Ricordiamo che :

- f:A $\to$A è invertibile se $\exists$ g:A $\to$A t.c. $f \circ g = Id_A$ e $g \circ f = Id_A$
- Se f è invertibile allora l'inversa è unica (coincide con g).



COMPOSIZIONE DI FUNZIONI
Se f: A$\to$B , g:B$\to$C allora:
g∘f : A$\to$C è definita da (g∘f)(a) = g(f(a)) $\forall a \in$ A

Quindi per provare che g è l'inversa di f basta verificare che valgono le due condizioni $f \circ g = Id_A$ e $g \circ f = Id_A$.

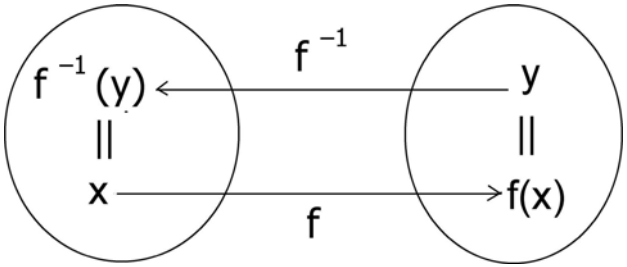
Indichiamo ZxZ con Z^2

- $f \circ g : Z^2 \to Z^2$ $f(g(a,b)) = f(b-1,b-a)$
  $= (b-1- (b-a) +1, (b-1)+1)$
  $= (a,b)$
  $\Rightarrow f \circ g = Id_{Z^2}$
- $g \circ f = Id_A$ $g(f(x,y)) = g((x-y+1, x+1))$
  $= ((x+1)-1, (x+1)-(x-y+1))$
  $= (x,y)$
  $\Rightarrow f \circ g = Id_{Z^2}$ OK

- QUANDO f È INVERTIBILE ?

  f:A→A è invertibile ⇔ f è bigettiva

- Com'è definita l'inversa f^{-1} di f , quando esiste ?



Se y∈R (codominio), la controimmagine di y tramite f è $f^{-1}(y)=\{x\in R \text{ (dominio)} \mid f(x)=y\}$,e se f è bigettiva,$f^{-1}(y)=\{x\}$ e ciò ci consente di definire la funzione inversa $f^{-1}(y)=x$

Attenzione: f^{-1} è un simbolo con duplice significato

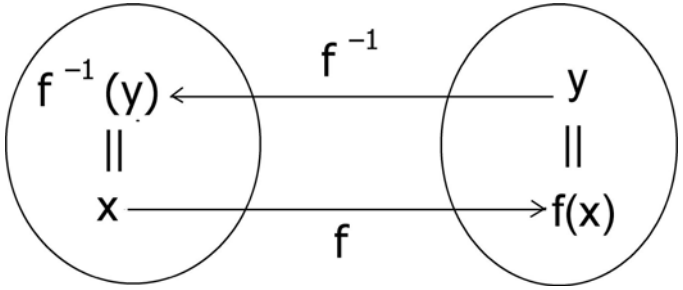
ESERCIZIO 4.

Determinazione dell'inversa

a) Determinare l'inversa della funzione f: R → R definita da f(x) = 2x-3.

b) Determinare l'inversa della funzione g:ZxZ→ZxZ definita da g(a,b)=(a-1,2a+b).

Se mostriamo che la controimmagine di ogni elemento y del codominio è un sottoinsieme del dominio costituito da **un solo elemento** (diverso dal vuoto), proviamo che f è bigettiva e troviamo simultaneamente anche la definizione della funzione inversa.



Quindi risolviamo l'equazione 2x-3 = y , dove possiamo supporre y noto e x incognita. Ricaviamo x= $\frac{y+3}{2}$ unica soluzione.

Conclusione: f è bigettiva e la sua inversa è la funzione g: R $\rightarrow$ R definita da g(y) = $\frac{y+3}{2}$. (La funzione inversa si indica spesso con f^{-1}).

c) g:ZxZ$\rightarrow$ZxZ definita da g(a,b)=(a-1,2a+b)

Poniamo (a-1,2a+b) = (x,y).

Deduciamo che $\begin{cases} a-1=x \\ 2a+b=y \end{cases}$.

Supponiamo x,y noti, a,b incognite che ricaviamo:

$$\begin{cases} a=x+1 \\ b=y-2a \end{cases} \Rightarrow \begin{cases} a=x+1 \\ b=y-2(x+1) \end{cases} \Rightarrow \begin{cases} a=x+1 \\ b=y-2x-2 \end{cases}$$

Per ogni (x,y)$\in$ ZxZ codominio esiste una ed una sola soluzione (a,b)$\in$ ZxZ dominio tale che g(a,b) =(x,y) , per cui g è bigettiva e la sua inversa è h(x,y) = (x+1,y-2x-2).

h

ESERCITAZIONE N.3

23 ottobre 2007

- Funzioni
- Cenni di calcolo combinatorio
- Relazioni d'equivalenza

ESERCIZIO 1.

Ancora sulle funzioni iniettive , surgettive

Sia f:RxR→RxR definita da f(x,y)= (x+y, 3x-3y)

a) Stabilire se f è iniettiva

b) Stabilire se f è surgettiva

b) Proviamo in questo caso a partire dallo studio della surgettività :

f(x,y)= (x+y, 3x-3y) è surgettiva se ∀ (a,b)∈RxR (codominio) ∃ almeno una coppia (x,y) ∈RxR t.c. f(x,y)=(a,b).

Dalla definizione di f ricaviamo che si tratta di stabilire se il sistema $\begin{cases} x + y = a \\ 3x - 3y = b \end{cases}$ nelle incognite x, y (con a , b considerati termini noti) ha ALMENO una soluzione.

Per riduzione : $\begin{cases} 3x + 3y = 3a \\ 3x - 3y = b \end{cases}$

$6x = 3a+b$

$$\Rightarrow \quad \begin{cases} x = \dfrac{3a+b}{6} \\ 3\dfrac{3a+b}{6} - 3y = b \end{cases}$$

$$\Rightarrow \quad = \ldots \begin{cases} x = \dfrac{3a+b}{6} \\ y = \dfrac{3a-b}{6} \end{cases}$$

$\Rightarrow$ Per ogni $(a,b) \in RxR$ $\exists\,!\ (x,y) \in RxR$ t.c. $f(x,y)=(a,b)$

L'esistenza di *almeno una soluzione* del sistema ci garantisce la *surgettività di f*, il fatto che poi tale soluzione sia anche unica ci garantisce l'iniettività di f.

CONCLUSIONE: f è bigettiva

ESERCIZIO 2.

Contiamo le funzioni...

Siano A ={1,2,3}, B={1,2,3,4}. Si considerino gli insiemi seguenti

a) X = {funzioni f: A →B}

b) Y = {funzioni iniettive f: A →B}

c) Z = {funzioni iniettive f: A →B tali che f(1)=1}

d) W = {funzioni surgettive f: A →B}

Dire quanti elementi hanno gli insiemi X, Y, Z, W.

a) f: {1,2,3}→ {1,2,3,4} è una funzione quando ad ogni elemento del dominio fa corrispondere uno ed un solo elemento del codominio.

Ad esempio:

f

1 → 3

2 → 2

3 → 3

f è individuata da una terna ordinata $(\bullet,*,\blacklozenge)$ di elementi del codominio (che possono anche essere ripetuti). Quante sono queste terne? Per ogni elemento abbiamo 4 scelte. In totale $4\cdot4\cdot4 = 4^3 = 64$. Quindi $|X|=64$.

In generale le funzioni da A in B sono $|B|^{|A|}$

dove con |A| indichiamo la cardinalità dell'insieme A.

b) f: {1,2,3}→ {1,2,3,4} funzione iniettiva: funzione che manda elementi distinti in elementi distinti.

Ad esempio:

f: {1,2,3}→ {1,2,3,4} t.c. 1 →3, 2 →4, 3 →1

f è individuata da una terna **ordinata** (•,∗,♦) di elementi **distinti** del codominio.

Quante sono queste possibili terne (f(1),f(2),f(3)) ?

Ci sono 4 scelte per il I° elemento f(1) che, una volta fissato, consente 3 scelte per il II°, e così ... 2 scelte per il III° (per l'iniettività!).

In totale le terne sono : 4 · 3 · 2 = 24. Quindi |Y|=24.

QUESITO

E' una domanda "equivalente" chiedere:

quante sono le possibili assegnazioni di medaglie (oro, argento, bronzo) in una gara a cui partecipano 4 concorrenti ?

Sì, perché...

Le funzioni iniettive f: A →B con A={1,2,3,...k}, |B|=n, (k ≤ n) si chiamano disposizioni (semplici) di n oggetti di classe k , con k ≤ n

(nel nostro esempio:k=3, n=4) e il loro numero è

$D_{n,k} = n \cdot (n-1) \cdot (n-2) \cdot \cdots (n-(k-1))$

$D_{4,3} = 4 \cdot 3 \cdot 2$ (3 fattori decrescenti consecutivi) .

(Cfr. lo schema riassuntivo alle pagine successive).

c) funzioni iniettive f: {1,2,3}→ {1,2,3,4} tali che f(1)=1.

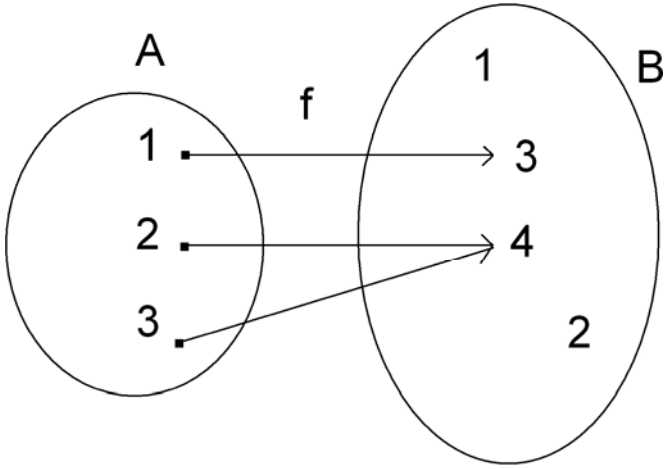
1 → 1

2 → ♣ abbiamo per ♣ 3 scelte (va escluso 1)

3 → ♠ abbiamo per ♠ 2 scelte (va escluso 1 e ♣)

Sono in pratica tante quante le funzioni iniettive di {2,3}→ {2,3,4}, cioè 3·2=6. Quindi |Z|=6.

d)



Im(f) ha al massimo 3 elementi

Se f fosse surgettiva sarebbe Im(f) = B, ma B ha 4 elementi e Imf ha al massimo 3 elementi : assurdo!

$\Rightarrow$ non ci sono f surg.

RIEPILOGO

Denominazione	Definizione	Numero
Disposizione con ripetizione	Funzione : A $\to$B A={1,2,3,...k}, |B|=n	n^k
Disposizione (semplice)	Funzione iniettiva: A $\to$B A={1,2,3,...k}, |B|=n, (k $\leq$ n)	n(n-1)(n-2)...(n-(k-1))
Permutazione	Funzione bigettiva: A $\to$A o funzione bigettiva f :{1,2,3,...,n}$\to$A, n=|A|	n!
Combinazione di classe k di n elementi , k$\leq$n	Sottoinsieme di {1,2,3,...n} di k elementi	$\binom{n}{k}$

ESERCIZIO 3.

... ancora un po' di calcolo combinatorio

a) Quanti sono i possibili anagrammi della parola "Esami" (senza tener conto del significato !) ?
b) Quanti modi ci sono di scegliere 5 giocatori di tennis da un team di 10 per partecipare ad un torneo?
c) Quante sono le possibili stringhe di bit di lunghezza sette?
d) Ciascun user di un sistema ha una password lunga da 6 a 8 caratteri, dove ogni carattere è una lettera minuscola o una cifra. Ogni password deve contenere almeno una cifra. Quante sono le possibili passwords ?

a) Sono tutti i possibili modi di "disporre",tenendo conto dell'ordine,i caratteri "e, s, a, m, i". Sono tanti quante le funzioni bigettive f:A={e,s,a,m,i}$\to$A={e,s,a,m,i},o eq.te g:A={1,2,3,4,5}$\to$ A={e,s,a,m,i},e son dette permutazioni di A.

Notiamo che nel caso finito per f:A$\to$ A si ha :
f bigettiva $\Leftrightarrow$ f iniettiva $\Leftrightarrow$ f surgettiva

Le permutazioni si possono riguardare come un caso particolare delle disposizioni (semplici), quando n=k.
Il n° delle permutazioni di un insieme di n elementi è:
n(n-1)(n-2) $\cdot \cdot \cdot$ 1 = n! (n fattoriale).
Nel nostro caso sono 5! = 5 $\cdot$ 4 $\cdot$ 3 $\cdot$ 2 $\cdot$ 1 = 120.

b) Contiamo le possibili cinquine scelte nell'insieme $L=\{1,2,3,4,.....,10\}$.

Poiché non conta l'ordine,ma solo gli elementi stessi (non ripetuti),sono tutti i possibili sottoinsiemi di 5 elementi di L.

Si chiamano "combinazioni" di classe k degli n elementi (qui k=5, n= 10) e sono

$$C_{n,k} = \binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-(k-1))}{k!} \quad (k \le n)$$

(al numeratore:k fattori decrescenti).

N.B. E' la formula $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ semplificata.

Nel ns.caso $C_{10,5} = \binom{10}{5} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5!} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 252.$

c) Ciascuno dei sette bits può essere scelto in due modi diversi, poichè ogni bit è zero o uno. Si tratta di contare tutte le funzioni f: $\{1,2,3,....,7\} \to \{0,1\}$. Sono quindi 2^7 .

d) Ci sono 26 lettere, 10 cifre. Il n° pwd P_6 con 6 caratteri è $P_6=36^6-26^6$

(= (n°pwd di lettere e/o cifre)–(n°pwd sole lettere))

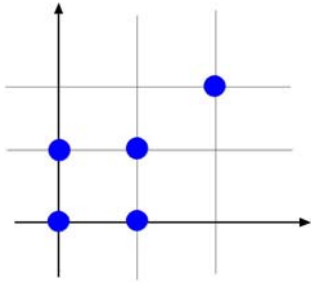
$P_7=36^7-26^7$, $P_8=36^8-26^8$ (in modo analogo).

Quindi: n°pwd totale=$P_6 + P_7 + P_8$=2.684.483.063.360 .

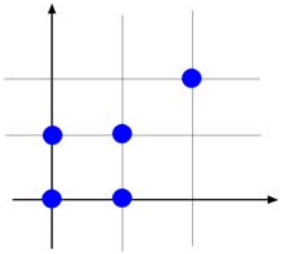
ESERCIZIO 4.

Relazioni binarie – relazioni d'equivalenza

La relazione disegnata è di equivalenza ?



RICORDIAMO CHE :



A = {0,1,2}

$\mathcal{R}=\{(0,0), (0,1), (1,0), (1,1), (2,2)\}$

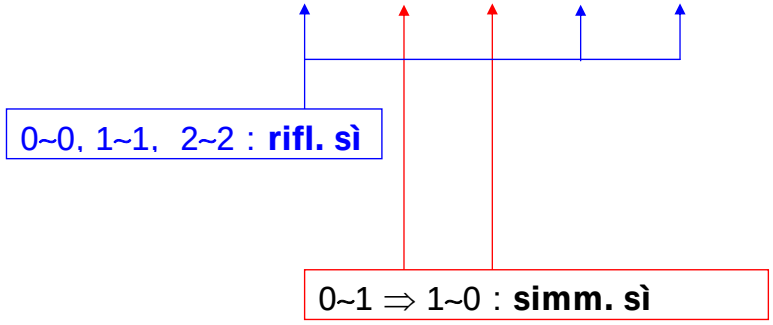
Una relazione binaria su un insieme A è un sottoinsieme del prodotto cartesiano AxA. Dati x, y elementi di A diciamo che x è in relazione con y e scriviamo $x \sim y$ (opp. $x \mathcal{R} y$) se $(x,y) \in AxA$.

- Una relazione $\sim$ su A è di equivalenza se è
  - riflessiva: $x \sim x$, $\forall\, x \in A$
  - simmetrica: $x \sim y \Rightarrow y \sim x$, $\forall\, x,y \in A$
  - transitiva: $x \sim y$ e $y \sim z \Rightarrow x \sim z$, $\forall\, x,y,z \in A$

Dal disegno si 'leggono' la riflessiva e la simmetrica.

Rispetto alla bisettrice del I° quadrante ...

$A = \{0,1,2\}$, $\mathcal{R}=\{(0,0), (0,1), (1,0), (1,1), (2,2)\}$



Transitiva: sì ! verificarlo !

ESERCIZIO 5.

Relazioni di equivalenza

Dire quali delle seguenti sono relazioni di equivalenza:

1. In ZxZ : $(a,b) \sim (c,d) \Leftrightarrow a=-c$
2. In Z: $a \sim b \Leftrightarrow a=b$ oppure $a=-b$
3. In R: $a \sim b \Leftrightarrow a \geq b$.

1. In ZxZ : $(a,b) \sim (c,d) \Leftrightarrow a=-c$

Non vale la riflessiva: $(1,0) \not\sim (1,0)$ perché $1 \neq -1$

2. In Z sia $a \sim b \Leftrightarrow a=b$ oppure $a=-b$

...in modo equivalente si può scrivere $a \sim b \Leftrightarrow |a|=|b|$

Quindi $\sim$ è rel. di equiv: l'uguaglianza in N è rel.di equiv.

3. In R sia $a \sim b \Leftrightarrow a \geq b$

Non vale la simmetrica :

$3 \sim 2$ perché $3 \geq 2$, ma $2 \not\sim 3$ poiché $2 \geq 3$ è falso

ESERCITAZIONE N.4

30 ottobre 2007

- Relazioni d'equivalenza
- Classi di equivalenza

ESERCIZIO 1.

Relazione di equivalenza su ZxZ

In ZxZ è data la corrispondenza

$(x,y) \sim (z,w) \Leftrightarrow 2(x-z)=5(y-w)$.

Provare che ~ è una relazione d'equivalenza

- Proviamo la riflessiva, ossia proviamo che ogni elemento di ZxZ è in relazione con se stesso:

$(x,y)\sim(x,y)$ per ogni $(x,y) \in ZxZ$.

Cosa vuol dire $(x,y)\sim(x,y)$?

Nella definizione questo x corrisponde a z	Nella definizione questo y corrisponde a w

Allora $(x,y)\sim(x,y)$ se e solo se risulta $2(x-x) = 5(y-y)$ ossia $0=0$, che è vero !

Quindi la proprietà riflessiva è provata per TUTTI gli elementi (x,y) del nostro insieme ZxZ.

- Proviamo la simmetrica :

dobbiamo verificare che se (x,y)~(z,w) allora (z,w)~(x,y)
per tutti gli (x,y),(z,w)∈ ZxZ

L' ipotesi è (x,y)~(z,w) che equivale a **2(x-z)=5(y-w)**.
La tesi è (z,w)~(x,y) che equivale a **2(z-x)=5(w-y)**.

Come si fa ad ottenere dall'uguaglianza 2(x-z)=5(y-w), l'uguaglianza 2(z-x)=5(w-y) ?
Basta cambiare di segno ! Allora è vera la tesi.

- Proviamo infine la transitiva:

dobbiamo verificare che se (x,y)~(z,w) e (z,w)~(p,q) allora (x,y)~(p,q) per tutti gli (x,y), (z,w), (p,q) ∈ ZxZ

Ipotesi : (x,y) ~ (z,w) che equivale a 2(x-z)=5(y-w) (1)
(z,w) ~(p,q) che equivale a 2(z-p)=5(w-q) (2)
Tesi : (x,y) ~ (p,q) che equivale a 2(x-p)=5(y-q) (3)

Come ottenere (3) da (1) e (2) ?
Sommando m. a m. (1) e (2) si ha (3), allora la tesi è vera.

UN MODO ALTERNATIVO DI MOSTRARE CHE ~ È REL. DI EQUIV.

Un caso in cui è 'rapido' verificare l'equivalenza di una corrispondenza è quando coincide con la relazione d'equivalenza associata ad una funzione.

Se f:A→B è una funzione, la relazione d'equivalenza associata ad f è $\mathcal{R}_f$:
In A $x \mathcal{R}_f y \Leftrightarrow f(x) = f(y)$.

Si tratta di individuare f .
In ZxZ: $(a,b) \sim (c,d) \Leftrightarrow 2(a-c)=5(b-d)$
Una funzione 'giusta' è f:ZxZ→A t.c. f(a,b)= f(c,d)∈A, con A insieme opportuno.
Trascrivo 2(a-c)=5(b-d) così : 2a-5b=2c-5d, e ora ponendo f(x,y) = 2x-5y risulta:

- f(a,b) = 2a-5b, f(c,d)=2c-5d
- essendo x,y,2,-5 interi ⇒2x-5y è intero⇒A=Z.

Dunque f:ZxZ → Z è definita da f(x,y)= 2x-5y.
E si ha (a,b)~(c,d)⇔f(a,b)=f(c,d).
Quindi la relazione ~ **coincide con** $\mathcal{R}_f$ ed è quindi una relazione d'equivalenza.

ESERCIZIO 2.

Classi di equivalenza

a) Data in Z la relazione di equivalenza

$a \sim b \Leftrightarrow a=b$ oppure $a=-b$

Descrivere le classi di equivalenza e stabilire se hanno lo stesso numero di elementi.

b) Data in RxR la relazione d'equivalenza

$(x,y) \sim (z,w) \Leftrightarrow 2(x-z)=5(y-w)$, determinare la classe di $(0,0)$ e la classe di $(\pi,2)$. Descrivere le classi.

a) In Z: $a \sim b \Leftrightarrow a=b$ oppure $a=-b$

Ricordiamo che un modo per provare che $\sim$ è una relazione d'equivalenza è notare che $\sim$ coincide con la relazione d'equivalenza $\mathcal{R}_f$ associata alla funzione

$f:Z\to Z$ definita da $f(x)=|x|$ (oppure $f:Z\to N$)

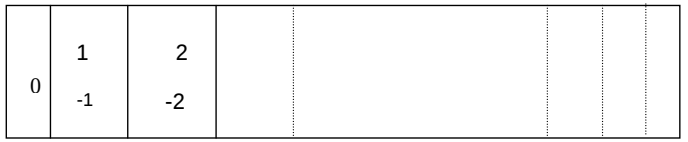
Descriviamo qualche classe, ad esempio $\bar{1}$ (classe di 1)

$\bar{1} = \{x\in Z \mid x\sim 1\} = \{x\in Z \mid x=1 \text{ oppure } x=-1\} = \{1,-1\}$

$\bar{0} = \{x\in Z \mid x\sim 0\} = \{0\}$

$\overline{-1} = \{x\in Z \mid x\sim -1\}$,ma $\overline{-1} = \bar{1}$ perchè $1 \sim -1$

$\bar{a} = \{x\in Z \mid x\sim a\} = \{x\in Z \mid x=a \text{ oppure } x=-a\} = \{a,-a\}$



Le classi hanno tutte due elementi, tranne la classe $\bar{0}$ che ne ha uno.

Le classi sono a due a due disgiunte e l'unione dà Z: ciò vale in generale , si dice che sono una partizione di Z.

L'insieme delle classi si chiama *insieme quoziente*.

Ad ogni relazione di equivalenza è associata una partizione e viceversa.

b) In RxR $(x,y)\sim(z,w) \Leftrightarrow 2(x-z)=5(y-w)$,

$\overline{(0,0)}$ (la classe di $(0,0)$) $=\{(x,y)\in RxR \mid (x,y)\sim(0,0)\}$

$=\{(x,y)\in RxR \mid 2(x-0)=5(y-0)\}$

$=\{(x,y)\in RxR \mid 2x-5y=0\}$

$=\{(x,\frac{2}{5}x)$, al variare di x in R$\}$

$\overline{(\pi,2)} = \{(x,y)\in RxR \mid (x,y)\sim(\pi,2)\}$

$= \{(x,y)\in RxR \mid 2(x-\pi)=5(y-2)\}$

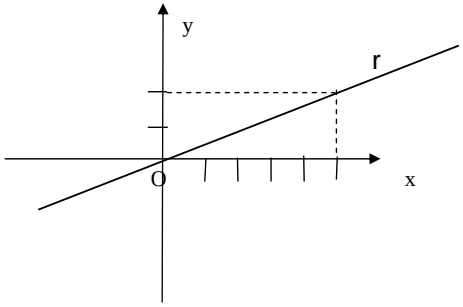
$= \{(x,y)\in RxR \mid 2x-5y-2\pi+10=0\}$

$= \{(x, \frac{2x-2\pi+10}{5}), \text{ al variare di x in R}\}$

Geometricamente:

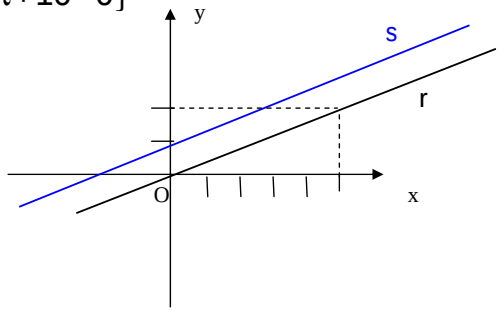
$\overline{(0,0)} = \{(x,y)\in RxR \mid 2x-5y=0\}$

È LA RETTA r DISEGNATA

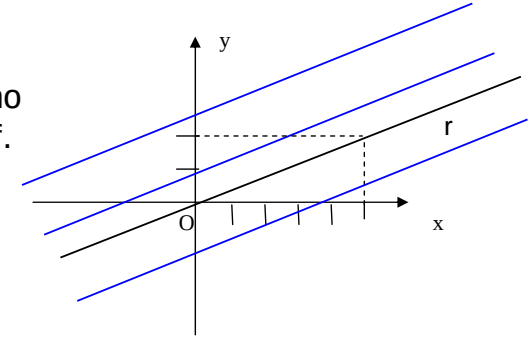


$\overline{(\pi,2)} = \{(x,y)\in RxR \mid 2x-5y-2\pi+10=0\}$

È una retta s parallela ad r: il coefficiente angolare è lo stesso di r ($m=-\frac{a}{b}=\frac{2}{5}$).



Le classi di equivalenza sono tutte rette parallele di coeff. angolare $\frac{2}{5}$.



ESERCIZIO 3.

Relazione di equivalenza in Q

Data in Q la corrispondenza

$x\sim y \Leftrightarrow x-y\in Z$

a) Verificare che ~ è una relazione d'equivalenza

b) Determinare la classe di 0 e la classe di $\frac{1}{3}$.

a)

- La prima proprietà da mostrare è che la corrispondenza è **riflessiva,** che vuol dire :

se x è un numero razionale (qualsiasi !), allora x è in relazione con se stesso.

Sappiamo come è definita la relazione: se $x-x\in Z$ allora $x\sim x$. Ora x-x vale zero, che appartiene a Z, quindi è vero che $x\sim x$.

- La seconda proprietà da mostrare è la **simmetrica**:

se x, y sono due qualsiasi numeri razionali e $x\sim y$, dobbiamo provare che allora $y\sim x$.

Per ipotesi $x \sim y$, e per come è definita la corrispondenza ciò vuol dire che $x-y \in Z$.
La tesi è : $y \sim x$, che sarà provata se mostriamo che $y-x \in Z$.
Dall'ipotesi abbiamo $x-y \in Z$, se ora cambiamo di segno al numero x-y, abbiamo il numero
$-(x-y) = -x+y = y-x$
che appartiene a Z, perché è l'opposto di x-y, che, per ipotesi sappiamo essere un numero intero.

- La terza proprietà è la **transitiva**:

ipotesi : $x \sim y$, $y \sim t$, con $x, y, t \in Z$
tesi: $x \sim t$
$x \sim y \Leftrightarrow x-y \in Z$ (1)
$y \sim t \Leftrightarrow y-t \in Z$ (2)

Sommiamo le informazioni :

$$(x-y)+(y-t) = x-t$$

$x-y \in Z$ per (1) $\qquad$ $y-t \in Z$ per (2)

Ma la somma di due numeri interi è ancora un numero intero e quindi $x-t \in Z$ e ciò equivale a $x \sim t$, la tesi è così provata.

b) La classe di 0 è per definizione l'insieme $\{x \in Q \mid x \sim 0\}$

e per def. di ~ si ha :

$$\{x \in Q \mid x \sim 0\} = \{x \in Q \mid x-0 \in Z\}$$
$$= \{x \in Q \mid x \in Z\}$$
$$= Z$$

QUINDI LA CLASSE D'EQUIV. DI 0 È Z

Analogamente la classe di $\frac{1}{3}$ è : $\{x \in Q \mid x \sim \frac{1}{3}\}$

$$= \{x \in Q \mid x-\frac{1}{3} \in Z\}$$
$$= \{x \in Q \mid x-\frac{1}{3} = n, \text{con } n \in Z\}$$
$$= \{x \in Q \mid x = \frac{1}{3}+n, \text{con } n \in Z\}$$

La classe di $\frac{1}{3}$ è quindi l'insieme di tutti i numeri razionali del tipo $\frac{1}{3} + n$ $(= \frac{1+3n}{3})$, con $n \in Z$

(ad esempio $\frac{1}{3}$, $\frac{4}{3} = \frac{1}{3}+1$, $-\frac{8}{3} = \frac{1}{3}-3$, , etc. sono tutti numeri che appartengono alla classe di $\frac{1}{3}$).

ESERCITAZIONE N.5

6 novembre 2007

- Divisione euclidea in Z
- Algoritmo euclideo per la determinazione del M.C.D.
- Identità di Bezout
- Equazioni diofantee lineari

Rosalba Barattero

ESERCIZIO 1.

La relazione "divide" in Z

E' data in Z^* la corrispondenza $x \sim y \Leftrightarrow$ x divide y.

Stabilire se è riflessiva, simmetrica, transitiva.

Diciamo che x divide y e scriviamo x|y se esiste $z \in Z^*$ tale che y=xz. Si può anche dire che x è un divisore di y, o che y è un multiplo di x.

Ad es. 2|12 perché $12=2 \cdot 6$, $3 \nmid 8$ (3 non divide 8) perché non esiste nessun $z \in Z^*$ tale che 8=3z.

RIFLESSIVA: a divide a ? Sì $a=1 \cdot a$

SIMMETRICA: Se a|b allora b|a ?

NO, 2 divide 12 ma 12 non divide 2

TRANSITIVA: Se a|b e b|c allora a|c ?

Ipotesi : $a|b \Rightarrow \exists\, c \in Z^*$ t.c. b=ac (1)

$b|c \Rightarrow \exists\, d \in Z^*$ t.c. c=bd (2)

Tesi : a|c cioè $\exists\, x \in Z^*$ t.c. c=ax

Da (2) c=bd, sostituendo (1) si ha : c=(ac)d=a(cd).

Quindi x=cd va bene. Perciò ~ è transitiva.

LA DIVISIONE EUCLIDEA IN Z

Siano a, b $\in$ **Z** , b$\neq$0. Allora esistono e sono unici due interi, il quoziente q e il resto r tali che a = b·q +r , con 0≤r<|b|.

Come si fa la divisione se entrambi o uno dei numeri a, b è negativo ?

Esempio 1 : -62 : 20 = ?
-62 = 20 (-3) – 2 Non va bene ! il resto è negativo !
-62 = 20(-4) + 18 OK !

Esempio 2: 62 : (-20) = ?
Si fa 62 = 20 · 3 +2, poi si cambia segno
…
62 = (-20) · (- 3) +2

Esempio 3: (-62) : (-20) = ?
(-62) = (-20) · 4 +18.

Vediamo un' applicazione dell'algoritmo della divisione.

ESERCIZIO 2.

Numeri di patente in Florida*

I numeri di patente in Florida sono codificati nel modo seguente SSSS-FFF-YY-DDD, dove nei gruppi con 'S' ed 'F' ci sono informazioni relative a nome e cognome, mentre YY indicano le ultime due cifre dell'anno di nascita e DDD codificano il mese m e il giorno b di nascita secondo la seguente espressione:
40(m-1)+b nel caso dei maschi,
40(m-1)+b+500 nel caso delle femmine.

Trascuriamo i casi di persone aventi lo stesso numero di patente, etc.

Determiniamo la data di nascita e il sesso dei titolari di patente aventi un numero di patente le cui ultime 5 cifre del codice sono: 80251, 62789.

80251: 80 indica l'anno di nascita 1980
251 corrisponde a 40(m-1)+b , poiché risulta
40(m-1)+b+500 ≥ 501. Si tratta quindi di maschio.
251 : 40 = ? 251= 40 · 6+11
6 è il quoziente e 11 il resto (univocamente determinati).
⇒ 80251 : maschio nato il giorno 11 luglio 1980

* Joseph Gallian – *Contemporary Abstract Algebra* – D.C. Heath and Company - 1994

62789: 62 indica l'anno di nascita 1962

789 corrisponde a 40(m-1)+b+500, poiché il massimo di 40(m-1)+b è 40 · 11 +31 = 471. Si tratta quindi di femmina.

789= 40(m-1)+b+500 $\Rightarrow$ 789-500= 40(m-1)+b

$\Rightarrow$ 289=40(m-1)+b

289 : 40 = ? 289= 40 · 7+9

7 è il quoziente e 9 il resto (univocamente determinati).

$\Rightarrow$ 62789 : femmina nata il giorno 9 agosto 1962.

Per approfondimenti su US Driver's License Numbers:

http://www.highprogrammer.com/alan/numbers/dl_us_shared.html

http://www.highprogrammer.com/alan/numbers/dl_us_shared_mmm.html

Qui un applet Java per codificare i dati della Florida

http://www.highprogrammer.com/cgi-bin/uniqueid/dl_fl

DEF. di M.C.D. (a,b) , con a, b interi non entrambi nulli:
è quell'intero d tale che

- d|a e d|b
- per ogni intero c tale che c|a e c|b, risulta c|d

Esempi :

- M.C.D. (12,18)= 6.

  L'insieme dei divisori comuni (positivi) è: {1,2,3,6},

  6 è il più grande dei divisori comuni, ed è anche multiplo di tutti i divisori.

  Anche -6 va bene, ma prendiamo quello positivo: intendiamo che in Z M.C.D. è unico a meno del segno.

- M.C.D. (10,0) = ? E' un caso particolare.

  Qualunque numero divide zero: $a \cdot 0=0 \ \forall a \in Z$.

  {1,2,5,10} è l'insieme dei divisori comuni , 10 è il M.C.D.(10,0).

ESERCIZIO 3.

M.C.D. con l'algoritmo euclideo e identità di Bezout

Calcolare il M.C.D. tra 88 e 34 con l'algoritmo di Euclide, e scrivere la corrispondente identità di Bezout.

L'algoritmo euclideo consiste in una sequenza di divisioni successive:

1. $88 = 34 \cdot 2 + 20$ ⟶ poiché il resto è $20 \neq 0$, procediamo
2. $34 = 20 \cdot 1 + 14$ dividendo il divisore 34 per il resto
3. $20 = 14 \cdot 1 + 6$ 20, e così via, fino ad avere resto
4. $14 = 6 \cdot 2 + 2$ nullo.
5. $6 = 2 \cdot 3$

L'algoritmo di Euclide afferma che l'ultimo resto non nullo è il M.C.D.(88,34). Abbiamo ritrovato M.C.D.(88,34)=2 .

Questo succede perché il M.C.D. tra dividendo e divisore di una divisione euclidea è uguale al M.C.D. tra divisore e resto. Così si ha: M.C.D.(88,34)=M.C.D.(34,20)=M.C.D. (20,14) = M.C.D.(14,6) = M.C.D.(6,2) = 2

Teorema di Bezout

Se d= M.C.D. (a,b), allora esistono due interi m, n tali che d= am +bn.

Scriviamo dunque 2 come combinazione lineare di 88 e 34, ossia cerchiamo due interi x e y tali che 88x +34y=2.
Alla tabella precedente affianchiamo a destra l'espressione dei resti:

1. $88 = 34 \cdot 2 + 20$	$20 = 88 - 34 \cdot 2$
2. $34 = 20 \cdot 1 + 14$	$14 = 34 - 20 \cdot 1$
3. $20 = 14 \cdot 1 + 6$	$6 = 20 - 14 \cdot 1$
4. $14 = 6 \cdot 2 + 2$	$2 = 14 - 6 \cdot 2$
5. $6 = 2 \cdot 3$	

Partiamo dalla riga 4.(quella in cui compare l'ultimo resto non nullo), e sostituiamo a ritroso i resti:

$2 = 14 - 6 \cdot 2$
$= 14 - (20 - 14 \cdot 1) \cdot 2 = 14 - 20 \cdot 2 + 14 \cdot 2 = 14 \cdot 3 - 20 \cdot 2$
$= (34 - 20 \cdot 1) \cdot 3 - 20 \cdot 2 = 34 \cdot 3 - 20 \cdot 3 - 20 \cdot 2 = 34 \cdot 3 - 20 \cdot 5$
$= 34 \cdot 3 - (88 - 34 \cdot 2) \cdot 5 = 34 \cdot 3 - 88 \cdot 5 + 34 \cdot 10 = 34 \cdot 13 - 88 \cdot 5$
$= 88\,(-5) + 34\,(13)$ OK !

CONCLUSIONE. M.C.D.(88,34)=2 & $2 = 88(-5) + 34(13)$

Osservazione a) se n indica il n° dei passi dell'algoritmo euclideo si ha : $n \leq 2\lg_2 b$. Qui $n \leq 2\lg_2 34 \approx 2 \cdot 5.08 \leq 11$
b) Un'altra maggiorazione [G. Lamé]: **$n \leq 5m$**, con m=n° cifre del minore tra i due numeri a e b. Qui **$n \leq 5 \cdot 2 = 10$**

EQUAZIONI DIOFANTEE LINEARI

(= equazioni di I° grado a coefficienti
in **Z** che vengono risolte in **Z**)

1 INCOGNITA

Esempi a) $3x=4$ non ha sol. in **Z**

b) $5x=10$ ha unica sol. in **Z**, $x= 10/5 =2$

Quindi $ax=b$ con $a, b \in \mathbf{Z}$, $a\neq 0$ ha un'unica soluzione in Z ($x= b/a$) se e solo se $a|b$ (a divide b)

Altrimenti **non** ci sono **soluzioni in Z**

2 INCOGNITE

Esempi a) $4x+6y=3$ **non** ha sol. in **Z**:comunque si sostituiscano x e y con due interi il I° membro è pari, il secondo è dispari.

Si noti che in **R** l'equazione ha infinite soluzioni, basta assegnare ad x un generico valore reale t e ricavare il corrispondente

$y= \dfrac{3-4t}{6}$, con $t\in R$.

b) $3x+6y=18$ **ha** soluzioni intere,ad esempio (4,1), (-6,6),(10,-2).

c) $88x+34y=2$ ha tra le sue soluzioni (-5,13): trovate nell'es.prec.

PROBLEMA 1. Stabilire se e quando $ax+by=c$ ha soluzioni in **Z**.

[Osservazione. Se c=0 esiste almeno la soluzione (0,0).]

RISPOSTA L'equazione $ax+by=c$, con $a,b,c\in \mathbf{Z}^*$

ha soluzioni in **Z** $\Leftrightarrow$ M.C.D. (a,b) divide c.

Dim. Se esiste la soluzione intera (x_0,y_0) allora si ha $ax_0+by_0=c$.
Se d è il M.C.D. (a,b) allora a=dr, b=ds, quindi sostituendo : $c= (dr)x_0+(ds)y_0 = d(rx_0+sy_0)$, che ci dice d divide c.
Viceversa supponiamo che d divida c, ossia $dm=c$.
Dalla proprietà del M.C.D.(a,b) si sa che esistono $x_0,y_0 \in \mathbf{Z}$ tali che $d= ax_0+by_0$. Quindi si ha: $c = dm= (ax_0+by_0)m = a(mx_0)+b(my_0)$
Questo ci dice che l'equazione diofantea $ax+by=c$ ha la soluzione $x= mx_0$, $y=my_0$ (o meglio la coppia (mx_0,my_0)).

ESERCIZIO4. Stabilire se l'equazione lineare $88x+34y=10$ ha soluzioni intere.

Per l'Ex.3 M.C.D.(88,34)=2. Poiché 2 divide 10, l'equazione ha soluzioni intere, per il risultato precedente.

Ma possiamo dire di più : nell'Ex. 3 si era trovato

$88(-5) + 34(13) = 2$

Se moltiplichiamo l'uguaglianza per 5 troviamo:

$88(-5\cdot 5) + 34(13\cdot 5) = 2\cdot 5$, che possiamo trascrivere così

$88(-25) + 34(65) = 10$. Questa uguaglianza ci dice che (-25,65) (x=-25, y=65) è soluzione di $88x+34y=10$!!

Abbiamo risposto al seguente

PROBLEMA 2. Nel caso in cui ax+by=c abbia soluzioni intere trovare una soluzione.

> **RISPOSTA.** Troviamo prima una soluzione di ax+by=d, d= M.C.D. (a,b), (ad esempio) con l'algoritmo di Euclide e poi la moltiplichiamo per c/d.

PROBLEMA 3. Nel caso in cui ax+by=c abbia soluzioni determinarle tutte.

> **RISPOSTA.** Sommiamo ad una sua soluzione tutte le soluzioni dell'*equazione omogenea associata*.
> (per la dim. cfr. dispense G.Niesi)

Lo terminiamo la prossima volta.

m

ESERCITAZIONE N.6

13 novembre 2007

- Equazioni diofantee lineari: applicazioni
- Il teorema fondamentale dell'aritmetica
- L'aritmetica dell'orologio di Gauss

ESERCIZIO 1.

Esercizio conclusivo sulle soluzioni delle eq.ni diofantee lineari

Stabilire se l'equazione 88x+34y=10 ha soluzioni intere e, se sì, determinarle.

1. M.C.D.(88,34)=2, 2 divide 10$\Rightarrow$ l'eq.^{ne} ha sol.^{ni} intere

2. Una soluzione particolare di ax+by=c, con a=88, b=34, c=10 è (-25,65).

   Abbiamo visto che si procede così:
   troviamo prima una soluzione di ax+by=d, dove
   d è il M.C.D. (a,b), con l'algoritmo di Euclide e l'identità di Bezout : 88(-5) + 34(13) = 2
   e poi la moltiplichiamo per c/d
   88(-5·5)+34(13·5)=2·5 $\Rightarrow$ 88(-25)+34(65)=10

3. L'equazione omogenea associata 88x+34y=0 ha i coefficienti non coprimi, allora si divide per il M.C.D.(88,34) =2, si ricava l'equazione 44x+17y=0, le cui infinite soluzioni sono (-17t, 44t) al variare di t in Z.

4. Si somma la soluzione generale dell'omogenea con la soluzione particolare e si determinano TUTTE le soluzioni di 88x+34y=10 :

(-17t,44t)+(-25,65)=(somma ordinata delle componenti)

= (-17t-25,44t+65) al variare di t∈Z .

CHIARIMENTI RELATIVI A 3.

STUDIO SOLUZIONI EQUAZIONE OMOGENEA ASSOCIATA

ax+by=0 è l'equazione omogenea associata all'equazione ax+by=c.

L'equazione ax+by=0 ha sempre la soluzione (0,0), anche (-b,a) è soluzione.

DOMANDA *E' vero che basta moltiplicare la soluzione non nulla trovata per un qualunque numero intero per avere tutte le infinite soluzioni ?*

Studiamo il ns. esempio 88x+34y=0:

(-34,88) è sol.^{ne}, vuol dire che risulta 88(-34)+34(88)=0, allora moltiplicando per un intero non nullo, ad es. 2 si ha 88(-34·2)+34(88·2)=0, da cui si ricava

(-34·2, 88·2)=(-68,176) è sol.^{ne} dell'eq.^{ne} 88x+34y=0 e così via ... (-34t,88t) al variare di t∈Z sono sol.^{ni}

⏩⏩Ma attenzione ! Da 88(-34)+34(88)=0 si osserva che, dividendo per 2, anche (-17,44) è sol.^{ne}, che non rientra però nelle soluzioni (-34t,88t) al variare di t∈Z :

NON c'è nessun valore intero di t che consenta di ottenere (-17,44) = (-34t,88t), perché dovrebbe essere

-17= -34t e 44 =88t , ma dalla prima segue $t=\frac{1}{2} \notin \mathbf{Z}$.

Quindi le coppie (-34t,88t) al variare di t∈**Z** sono sì soluzione dell'equazione 88x+34y=0 ma **non** sono **TUTTE** le infinite soluzioni !

⏩⏩ E' necessario riscrivere l'equazione 88x+34y=0, riducendola ai minimi termini,tramite la semplificazione per 2, così **44x+17y=0**.

Ora M.C.D.(44,17)=1 (44 e 17 sono *coprimi , primi fra loro*) ed è **corretto** dire che tutte le soluzioni sono

x= -17t, y=44t , t∈Z !

Perché ?

In virtù del seguente

LEMMA DI EUCLIDE

In Z se a divide bc, e se M.C.D.(a,b)=1, allora a divide c.

N.B. L'ipotesi M.C.D.(a,b)=1 è essenziale!
Ad es. siano a= 6, b=4, c=15, si ha: 6 divide 4·15 (=60), infatti 6·10=60 ma 6 non divide nè 4, nè 15.

Il procedimento per ricavare le soluzioni funziona così : da 44x+17y=0, o 44x= -17y si deduce che: 44 divide -17y , e M.C.D.(44,17)=1, allora per il lemma di Euclide 44 divide y e quindi $\exists$ t$\in$Z t.c. y=44t, da cui per sostituzione nell'eq.^{ne} 44x+17y=0 si ha 44x+17(44t)=0 e semplificando si ricava x=-17t.

In conclusione tutte le soluzioni di ax+by=0 si trovano così:

- Si determina M.C.D.(a,b)=d
- Si divide per d l'equazione ax+by=0, ottenendo l'equazione equivalente (con le stesse soluzioni) $\alpha x+\beta y=0$, ($\alpha=\frac{a}{d}, \beta=\frac{b}{d}$),i cui coefficienti sono coprimi
- la soluzione generale in **Z** di ax+by=0 è la soluzione generale di $\alpha x+\beta y=0$: "scambiando in croce": **$x=-\beta t, y=\alpha t$** al variare di t in Z,(o equivalentemente) l'insieme $S=\{(-\beta t, \alpha t) | t\in Z\}$.

ESERCIZIO 2.

Il problema dei 100 polli di Chang Chhiu-Chien

Se un gallo costa 5 monete, una gallina 3 monete e con una moneta si possono comprare 3 pulcini, quanti galli, galline e pulcini si possono comprare con 100 monete , volendo comprare in tutto 100 polli ?

Indichiamo : x= numero dei galli
y= numero delle galline
z= numero dei pulcini

Il quesito si traduce nel sistema $\begin{cases} x+y+z=100 \\ 5x+3y+\frac{1}{3}z=100 \end{cases} \Rightarrow$

$$\begin{cases} z=100-x-y \\ 5x+3y+\frac{1}{3}(100-x-y)=100 \end{cases} \Rightarrow \begin{cases} z=100-x-y \\ 14x+8y=200 \cdot \end{cases}$$

La seconda equazione è una diofantea lineare che possiamo semplificare in 7x+4y=100.
Una soluzione particolare si vede essere (0,25).

L'eq.omog.ass. 7x+4y=0 ha i coefficienti che sono **primi fra loro**, perciò le sue infinite soluzioni sono (4t,-7t) al variare di t∈Z, e di conseguenza la soluzione generale dell'equazione 14x+8y=200 è

(0,25)+ (4t,-7t) = (4t, 25-7t) al variare di t∈Z , quindi la soluzione del sistema è

x= 4t, y= 25-7t, z= 75+3t al variare di t∈Z.

Chang Chhiu-Chien,nel suo trattato di ″Matematica classica″ (~250 d.C.) dà le risposte

x=4	y=18	z=78
x=8	y=11	z=81
x=12	y=4	z=84

Infatti occorre mettere la condizione di positività !

$4t > 0; \quad 25 - 7t > 0; \quad 75 + 3t > 0$

$t > 0 \qquad -25 < t < 3 + \frac{4}{7}$

Quindi per t=1,2,3 si ottengono le soluzioni di Chang !

ESERCIZIO 3.

Sulle funzioni

Sia f:ZxZ→Z la funzione definita da f(x,y)=6x-15y.

a) Determinare $f^{-1}(0)$ e $f^{-1}(12)$.

b) Stabilire se f è iniettiva, surgettiva.

a) $f^{-1}(0)=\{(x,y)\in ZxZ \mid f(x,y)=0\}= \{(x,y)\in ZxZ \mid 6x-15y=0\}$.

Semplificata per 3 l'equazione si riduce a 2x-5y=0,

ossia 2x=5y, i cui coefficienti sono primi fra loro.

Ora si può procedere come sempre: M.C.D.(2,5)=1,quindi 2 divide y, ossia y= 2t , da cui segue x=5t , con t∈Z.

Si ottiene $\mathbf{f^{-1}(0) = \{(5t,2t) \mid t\in Z\}}$.

$f^{-1}(12)=\{(x,y)\in ZxZ \mid f(x,y)=12\}=\{(x,y)\in ZxZ \mid 6x-15y=12\}$.

Una soluzione particolare di 6x-15y=12 è (-3,-2).

La soluzione generale è (-3,-2)+(5t,2t)=(-3+5t,-2+2t),t∈Z

Si ottiene $\mathbf{f^{-1}(12) =\{(-3+5t,-2+2t) \mid t\in Z\}}$.

b) Si può avere $f^{-1}(\clubsuit)= \{(x,y)\in ZxZ \mid 6x-15y=\clubsuit\} = \varnothing$?

6x-15y=c ha soluzioni in Z ⇔ M.C.D.(6,15) divide c

M.C.D.(6,15)=3,ad es.non ci sono soluzioni se c=2.Così $f^{1}(2)=\varnothing$ ed f **NON** è **surgettiva**.

Da a) f **NON** è **iniettiva:** $f^{-1}(0)$ ha infiniti elementi ((0,0)≠(5,2) ma f(0,0)=f(5,2)= 0).

ESERCIZIO 4. (*)

Contiamo i divisori

Qual è il più piccolo numero naturale che possiede esattamente 20 divisori (positivi), contando anche 1 e il numero stesso ?

(A) $2^9 \cdot 3$

(B) 2^{19}

(C) 2^{20}

(D) 240

(E) nessuno dei precedenti

Occorre applicare il *teorema fondamentale dell'aritmetica:*

Ogni numero intero n>1 è il prodotto di un numero finito di fattori primi. Tale fattorizzazione è unica a meno dell' ordine dei fattori.

Un numero *primo* è un numero naturale maggiore di 1 che è divisibile solo per 1 e per sè stesso (si intende divisori>0)

(B) 2^{19} è decomposto in fattori primi, contiamo i suoi divisori : $1, 2, 2^2, 2^3, \ldots, 2^{19}$, quindi sono 20.

(C) 2^{20} : analogamente ha 21 divisori

(*) Tratto da : PROGETTO OLIMPIADI DI MATEMATICA - SEZIONE DI ROMA – Gara a squadre – 23 marzo 2007
http://olimpiadi.ing.unipi.it/

(A) $2^9 \cdot 3$: per l'esponente relativo al 2 ci sono 10 scelte (da 0 a 9 : $2^0=1, 2^1, 2^2, \ldots, 2^9$), per l'esponente relativo al 3 ci sono 2 scelte (0,1 corrispondenti a $3^0=1, 3^1=3$).

$1 \cdot 1$	$1 \cdot 3$
$2 \cdot 1$	$2 \cdot 3$
$2^2 \cdot 1$	$2^2 \cdot 3$
...	
$2^9 \cdot 1$	$2^9 \cdot 3$

Quindi in tutto $10 \cdot 2 = 20$ scelte, e di conseguenza 20 divisori.

(D) 240 va decomposto in fattori primi :

$240 = 24 \cdot 10 = 2^3 \cdot 3 \cdot 2 \cdot 5 = 2^4 \cdot 3 \cdot 5$

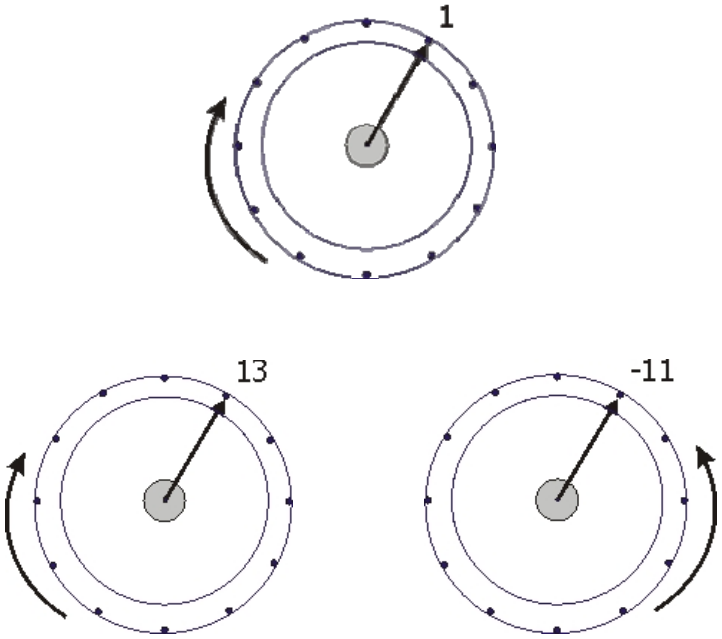
Come prima ricaviamo che il numero dei divisori di 240 è :$(4+1)(1+1)(1+1) = 20$

Ora basta confrontare i numeri $2^9 \cdot 3$, 2^{19}, 240 per concludere che il minore è 240.

[*Domanda-digressione*: quale è il M.C.D. $(2^9 \cdot 3, 2^{19})$?

M.C.D. $(2^9 \cdot 3, 2^4 \cdot 3 \cdot 5)$? ... fattori comuni con il minimo esponente.]

Il calcolatore ad orologio di Gauss (*)



1, 13, -11 , ... sono tra loro equivalenti (modulo 12)

- $9+4 = 13$, ma il calcolatore ad orologio di Gauss dà come risultato 1, scriviamo $9+4 \equiv 1$
- $7\cdot7 = 49$, ma il calcolatore ad orologio di Gauss dà come risultato 1 , ossia il resto di 49:12 $\Rightarrow 7\cdot7 \equiv 1$

(*) Parte di questa esposizione è tratta dal libro *'L'enigma dei numeri primi'* di Marcus Du Sautoy , BUR 2004

- $7\cdot7\cdot7 = ...$ invece di fare $49\cdot7$, Gauss può limitarsi a fare $1\cdot7$ e ottenere così 7 . L'informazione ottenuta dice che 7 è il resto di $7\cdot7\cdot7$ (=343, ma non occorre saperlo!) diviso per 12 $\Rightarrow 7\cdot7\cdot7 \equiv 7$
- $7^{99} = ?$ il calcolatore ad orologio dà come risultato 7, che vuol dire il resto di 7^{99}: 12 è 7 $\Rightarrow 7^{99} \equiv 7$

  Perché ? sappiamo che $7\cdot7 \equiv 1$, ossia $7^2 \equiv 1$, notiamo che possiamo scrivere

  $7^{99} = 7^{98}\cdot7 = (7^2)^{49}\cdot7 \Rightarrow 7^{99} \equiv (1)^{49}\cdot7 \equiv 7$

  Senza sapere quanto fa 7^{99} Gauss sa che il numero 7^{99} diviso per 12 dà resto 7 !

Gauss formalizza il tutto e così nasce la

➢ **DEFINIZIONE DI CONGRUENZA MODULO n**

Sia $n \in \mathbb{N}$. Due numeri interi $a, b \in Z$ si dicono congruenti modulo n, in simboli

$$a \equiv b \pmod{n}$$

se n divide la differenza a-b,ossia se vale $a-b=kn$ con $k \in Z$.

Lo studente F. osserva che si può generalizzare così : $7^{pari} \equiv 1$, $7^{dispari} \equiv 7$.

- *La congruenza è una relazione di equivalenza* e si può esprimere anche così :

  a, b ∈ Z sono congruenti modulo n

  se hanno lo **stesso resto** quando vengono divisi per n

Per ogni x∈Z vale **x ≡ r** dove r è il **resto** della divisione x:n

I resti possibili sono 0,1,2,3,4,...,n-1, quindi :

- ci sono **n classi di equivalenza.**

Nel caso n=12

$\bar{0}$ = {tutti gli elementi congruenti a 0}

= {...,-24,-12,0,12,24,... }

$\bar{1}$ = {tutti gli elementi congruenti a 1}

= {...,-23,-11,1,13,25,... } etc.

Le classi sono in tutto 12 : $Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, ..., \overline{11}\}$.

Ma gli orologi con 12 ore non hanno nulla di speciale !

Gauss crea così l'aritmetica modulare ('orologi' con un n. qualsiasi di ore).

t

ESERCITAZIONE N.7

20 novembre 2007

- Calcoli in Z_n
- Criteri di divisibilità
- Il piccolo teorema di Fermat

ESERCIZIO 1.

L'orologio: la congruenza modulo 12

a) Per ciascuno dei numeri seguenti determinare il minimo intero positivo modulo 12 a cui è congruente:
19, -11, 149.

b) Se adesso sono le ore 14 (= 2 P.M.) che ora del giorno (o della notte) sarà tra 1000 ore ?

c) Se lo scorso anno Natale era di Lunedì, in che giorno cadrà Natale quest'anno e nel 2020 ?

a)

$19 \equiv ?\ (\mathrm{mod}\ 12)$

$19 = 12+7 \Rightarrow 19 \equiv 7\ (\mathrm{mod}\ 12)$ (pensare all'orologio!)

$-11 \equiv ?\ (\mathrm{mod}\ 12)$

$-11 = -12+1 \Rightarrow -11 \equiv 1$ ('giriamo in senso antiorario')

$149 \equiv ?\ (\mathrm{mod}\ 12)$ $149 = 12 \cdot 12 + 5 \Rightarrow 149 \equiv 5$

b) Se adesso sono le ore 14 (= 2 P.M.) che ora del giorno (o della notte) sarà tra 1000 ore ?

Dovremo determinare quel numero x , $0 \le x < 24$ tale che $\bar{x} = \overline{14+1000}$ mod (24).

$\bar{x} = \overline{1014} = \overline{42 \cdot 24 + 6} = \bar{6}$

↑ 1014: 24 = 42 con resto 6

Risposta: saranno quindi le 6 del mattino.

c) Se lo scorso anno Natale era di lunedì, in che giorno cadrà Natale quest'anno? e nel 2020 ?

Il 2007 ha 365 giorni (anno non bisestile).Poniamo:

0 = domenica , 1= lunedì, 2=martedì,3=mercoledì, 4= giovedì, 5= venerdì, 6= sabato

Troviamo x, $0 \le x < 6$ tale che $\bar{x} = \overline{1+365}$ mod 7

$\bar{x} = \overline{366} = \overline{7 \cdot 52 + 2}$ (366=7·52+2 in Z), quindi $\bar{x} = \bar{2}$.

Allora quest'anno Natale cade di Martedì.

Per il 2020 attenti al n° di anni bisestili (quelli divisibili per 4, ossia le ultime due cifre sono divisibili per 4: ce ne sono 4)

$\bar{x} = \overline{2 + 365 \cdot 13 + 4} = \ldots = \bar{5} \Rightarrow$ Natale 2020 è venerdì

OSSERVAZIONE

Per effettuare il calcolo $\overline{2 + 365 \cdot 13 + 4} = \bar{5}$ non occorre fare il calcolo 'sotto' la barra, trovare $\overline{5115}$, poi dividere 5115 per 7 e stabilire così che il resto è 5 !

Si può procedere così in Z_7 (senza uso di calcolatrici) :

$$\begin{aligned}\overline{2 + 365 \cdot 13 + 4} &= \overline{2 + (364 \cdot 13 + 1 \cdot 13) + 4} \\ &= \bar{2} + \overline{364 \cdot 13} + \overline{13} + \bar{4} \\ &= \bar{2} + \bar{0} + \overline{13} + \bar{4} \\ &= \overline{19} \\ &= \bar{5}\end{aligned}$$

52·7·13 : multiplo di 7

Questo é lecito farlo perché in Z_n valgono tutte le buone proprietà di Z

- def. di somma in Z_n : $\bar{a} + \bar{b} = \overline{a+b}$
- def. di prodotto in Z_n : $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$
- $\bar{0}$ è l'el. neutro risp. alla somma in Z_n cioè $\bar{a} + \bar{0} = \bar{a}$ per ogni $\bar{a} \in Z_n$, con $\bar{0} = \{\ldots -2n, -n, 0, n, 2n, \ldots\}$ e quindi $\bar{0} = \bar{n} = \overline{2n} = \ldots = \overline{kn}$ per ogni $k \in Z$
- $\bar{1}$ è l'el. neutro risp. al prodotto
- $\bar{a}$ ha opposto (risp. alla somma) $-\bar{a}$ (= $\overline{-a}$)
- potenza in Z_n : $\bar{a}^n = \overline{a^n}$
- Proprietà comm., ass. rispetto alla somma, etc.

QUALCHE CRITERIO DI DIVISIBILITÀ

2, 3,5,**7**,9,10,11

Il resto di 5567 diviso per 7 è …

Usiamo la consueta rappresentazione decimale (in base 10) dei numeri, le cui cifre sono interi compresi tra 0 e 9.

$5567 = 10^0 \cdot 7+10^1 \cdot 6+10^2 \cdot 5+10^3 \cdot 5$

Il numero $a_n .. a_2 a_1 a_0$ (scritto *in forma decimale)* è l'intero $10^0 \cdot a_0+10^1 \cdot a_1+10^2 \cdot a_2+..+10^n \cdot a_n$, dove $0 \le a_i \le 9$, i =0,..n.

Calcoliamo le potenze di 10 modulo 7:

$$10^0 \equiv 1 \pmod 7$$
$$10^1 \equiv 3 \pmod 7$$
$$10^2 \equiv 3^2 \equiv 2 \pmod 7$$
$$10^3 \equiv 3 \cdot 2 \equiv -1 \pmod 7$$
$$10^4 \equiv 3 \cdot (-1) \equiv -3 \pmod 7$$
$$10^5 \equiv 3 \cdot (-3) \equiv -2 \pmod 7$$
$$10^6 \equiv 3 \cdot (-2) \equiv 1 \pmod 7$$
$$10^7 \equiv 3 \cdot 1 \equiv 3 \pmod 7$$
$$\ldots$$

I resti si ripetono ciclicamente, è sufficiente conoscere i primi 6 coefficienti per comporre la serie di resti delle potenze di 10:

1,3,2,-1,-3,-2,……

$a_n .. a_2 a_1 a_0 \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + .. \pmod 7$

e di conseguenza nel caso particolare che il resto sia zero, esprimiamo così il criterio di divisibilità per 7:

7 divide $m = a_n .. a_2 a_1 a_0$ se e solo se

7 divide $a_0+3a_1+2a_2-a_3-3a_4-2a_5+a_6+\ldots$.

Nel nostro caso: (scriviamo con le classi, è la stessa cosa)

$$\overline{5567} = \overline{a_0 + 3a_1 + 2a_2 - a_3} = \overline{7 + 3 \cdot 6 + 2 \cdot 5 - 5} = \overline{2}$$

$\Rightarrow$ Il resto di $239 \cdot 19$: 7 è 2 !!

Con lo stesso metodo si trovano i criteri di divisibilità per 2, 3, 5, 9, 10, 11

- 2 divide m se e solo se 2 divide a_0, quindi se e solo se a_0=numero pari
- 3 divide m se e solo se 3 divide $a_0 + a_1 + \ldots + a_n$
- 5 divide m se e solo se 5 divide a_0, quindi se e solo se a_0=0 oppure a_0=5
- 9 divide m se e solo se 9 divide $a_0 + a_1 + \ldots + a_n$
- 10 divide m se e solo se a_0=0
- 11 divide m se e solo se 11 divide $a_0 - a_1 + a_2 + \ldots + (-1)^n a_n$
- 4 divide m se e solo se 4 divide il numero rappresentato dalle due ultime cifre
  (cfr. http://www.dima.unige.it/~baratter/111111_o.pdf)

ESERCIZIO 2 .

Calcoli in Z_n

a) E' divisibile per 26 il numero $3^{12} - 1$?

b) Sia n=293·19. Determinare il resto della divisione di n per 7 ?

c) Sia n=1! + 2! + 3! +…+100! . Determinare il resto della divisione di n per 12.

d) Con quale cifra termina il numero 333^{222} ?

a) $(3^{12} - 1)$ è divisibile per 26 $\Leftrightarrow$
$(3^{12} - 1) = 26\,h$ con $h \in Z$ $\Leftrightarrow$(passando alle classi)
$\overline{3^{12} - 1} = \bar{0}$ in Z_{26} $\Leftrightarrow$(somma e opposto in Z_n)
$\overline{3^{12}} = \bar{1}$ in Z_{26}

Con un po' di esercizio si possono semplificare i calcoli.
Notiamo che in Z_{26} $\bar{3}^2 = \bar{9}$, $\bar{3}^3 = \bar{1}$.

Ma analizziamo bene i singoli passaggi in Z_{26} :

$\bar{3}^3 = \overline{3^3}$ (def. di potenza in Z_n)

$= \overline{27} = \overline{26+1}$ ("sotto la barra" siamo in Z)

$= \overline{26} + \bar{1}$ (somma in Z_{26})

$= \bar{0} + \bar{1} = \bar{1}$ ($\bar{0}$ è l'el. neutro risp. alla somma in Z_n).

Ora, sapendo che $\bar{3}^3 = \bar{1}$, eleviamo ambo i membri alla quarta, così otteniamo $(\bar{3}^3)^4 = \bar{1}^4$ e poiché valgono le solite proprietà delle potenze, concludiamo che $\bar{3}^{12} = \bar{1}$.

b) n=293·19. Quale è il resto della divisione di n per 7 ?

Per dire quale è il resto dobbiamo trovare $\bar{a} = \overline{293 \cdot 19}$ con a tale che $0 \le a < 7$ (a è l'unico che ha questa proprietà).

Calcoliamo in Z_7 :

$\overline{293 \cdot 19} = \overline{293} \cdot \overline{19}$ (def. prodotto in Z_7)

Dividiamo per 7 : $293 = 41 \cdot 7 + 6$, $19 = 2 \cdot 7 + 5$

passiamo alle classi in Z_7 : $\overline{293} = \overline{41 \cdot 7 + 6} = \bar{6}$,

$\overline{19} = \overline{2 \cdot 7 + 5} = \bar{5}$

Quindi $\overline{293 \cdot 19} = \bar{6} \cdot \bar{5} = \overline{30}$

Riduciamo ancora modulo 7 : $\overline{30} = \bar{2}$.

Finito : 2 è il resto di (293·19) : 7

c) Sia n=1! + 2! + 3! +…+100! . Determinare il resto della divisione di n per 12.

Per def. si ha a! = a(a-1)(a-2)···1, quindi

1!=1, 2!=2·1=2, 3! = 3·2·1=6, 4!=4·3·2·1=24 stop !

24 è multiplo di 12 e così sono i fattoriali successivi, perché 5!=5· 4! , 6!=6· 5! etc… n!=n (n-1)!

Quindi in Z_{12} si ha : $\bar{n} = \overline{1!+2!+3!+4!\ldots+100!}$

$= \bar{1}+\bar{2}+\bar{6}+\bar{0} = \bar{9}$

Per def. di somma negli Z_n

Poiché 9 è minore di 12, 9 è il resto di n:12.

d) Con quale cifra termina il numero 333^{222} ?

Ogni intero è congruo all'ultima cifra (le unità del numero nella sua rappresentazione decimale) modulo 10.

Quindi si fa il calcolo in Z_{10}.

…comodo con i negativi!

$\overline{333^{222}} = \overline{3^{222}}$ (perché $\overline{333}=\bar{3}$)

$= \overline{(3^2)^{111}}$ (ma in Z_{10} $\overline{3^2}=\overline{-1}$) $= \overline{(-1)^{111}} = \overline{-1} = \bar{9}$

Finito ! 9 è il resto di 333^{222} :10 e quindi 9 è l'ultima cifra.

ESERCIZIO 3 .

Il piccolo teorema di Fermat

Utilizzando il piccolo teorema di Fermat si calcoli il resto della divisione tra 5^{75} e 13.

La domanda è trovare il resto della divisione di 5^{75} per 13, per il teorema di divisibilità,dati a ed n interi (qui è n>o) sappiamo che

esistono unici q ed r, 0≤r<13 t.c. a=nq+r

⇔ " " " a – r = nq

⇔ " " " a ≡ r

⇔ " " " $\bar{a} = \bar{r}$

⏩ il resto r della divisione di a per n è l'unico intero 0≤r<n tale che $\bar{a} = \bar{r}$ in Z_n

Fissati $a=5^{75}$,n=13, cerchiamo dunque l'unico intero r, 0≤r<13 tale che $\bar{a} = \bar{r}$.

$5^{75} = 13 \cdot q + r$, $0 \le r < 13$ e passando alle classi in Z_{13} :

$$\overline{5^{75}} = \overline{13 \cdot q + r} = \overline{13 \cdot q} + \bar{r} = \overline{13} \cdot \bar{q} + \bar{r} = \bar{r}$$

$\overline{a+b} = \bar{a} + \bar{b}$ $\quad$ $\overline{a \cdot b} = \bar{a} \cdot \bar{b}$ $\quad$ $\overline{13} = \bar{0}$ in Z_{13}

PICCOLO TEOREMA DI FERMAT

Se p è un numero primo, e a è un intero non nullo e non divisibile per p, allora si ha $\bar{a}^{p-1} = \bar{1}$ ***in*** Z_p .

Qui p=13 primo, a=5 è un intero non nullo e non divisibile per 13, allora il Teorema ci dice che $\bar{a}^{p-1} = \bar{5}^{12} = \bar{1}$ in **Z_{13}** .

Pobbiamo utilizzare l'informazione $\bar{5}^{12} = \bar{1}$ in Z_{13} per calcolare 5^{75} :

$\bar{5}^{75} = \bar{5}^{12 \cdot 6 + 3}$ ← Dividiamo 75 per **12** a livello degli esponenti

$= \bar{5}^{12 \cdot 6} \cdot \bar{5}^{3}$ ← Proprietà delle potenze

$= \left(\bar{5}^{12}\right)^{6} \cdot \bar{5}^{3}$ ← Proprietà delle potenze

$= \left(\bar{1}\right)^{6} \cdot \bar{5}^{3}$ ← $\bar{5}^{12} = \bar{1}$ in Z_{13}

$= \bar{5}^{3}$ $(= \bar{5} \cdot \bar{5} \cdot \bar{5} = \overline{5 \cdot 5 \cdot 5} = \overline{5^3})$ $= \overline{125}$

Possiamo fermarci qua e dire che il resto della divisione di 5^{75} per 13 è 125 ? NO ! perché cerchiamo $\bar{5}^{75} = \bar{r}$ in Z_{13} , con $0 \le r < 13$.

Quindi $\bar{5}^{3}$ va ridotto modulo 13.

$\bar{5}^{3} = \bar{5} \cdot \bar{5} \cdot \bar{5}$

$= \overline{25} \cdot \bar{5}$

$= \overline{-1} \cdot \bar{5}$ (meglio così che $\overline{12} \cdot \bar{5}$)

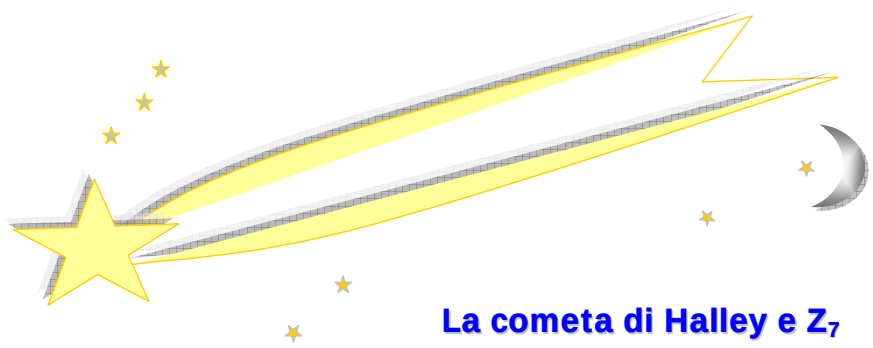
$= \overline{-5}$ (trasformiamo in rappresentante positivo: r≥0 !)

$= \bar{8}$

Risulta : $0 \le 8 < 13$ $\Rightarrow$ il ***resto*** della divisione di 5^{75} per 13 è ***8***

THE END

ESERCIZIO 4.



La cometa di Halley e Z_7

Le ultime tre apparizioni della cometa di Halley sono state negli anni 1835, 1910, 1986 e la prossima sarà nel 2061. Tra questi quattro numeri c'è il legame seguente

$$\overline{1835}^{1910} + \overline{1986}^{2061} = \bar{0} \quad \text{in } Z_7$$

Verifichiamolo !
Facciamo le seguenti divisioni:

- $1835 = 7 \cdot 262 + 1$
- $1986 = 7 \cdot 283 + 5$

Così riduciamo le basi modulo 7: $\overline{1835} = \bar{1}$, $\overline{1986} = \bar{5}$.

L'uguaglianza da verificare si è semplificata così:

$$\bar{1}^{1910} + \bar{5}^{2061} = \bar{0} \quad \text{in } Z_7$$

Per la proprietà delle potenze negli Z_n si ha : $\bar{1}^{1910} = \overline{1^{1910}} = \bar{1}$
Resta ancora da calcolare $\bar{5}^{2061}$, che deve valere $\bar{6}$.

Si può applicare il piccolo teorema di Fermat ?

Qui p=7 primo, a=5 è un intero non nullo e non divisibile per 7, allora il Teorema ci dice che $\bar{a}^{p-1} = \bar{5}^{6} = \bar{1}$ in Z_7 .

Per utilizzare questa informazione e calcolare $\bar{5}^{2061}$ $(= \overline{5^{2061}})$ è sufficiente fare la divisione per 6 ad esponente, e usare le solite proprietà delle potenze in Z

$$\begin{aligned}
\overline{5^{2061}} &= \overline{5^{343\cdot 6+3}} \\
&= \overline{5^{343\cdot 6}} \cdot \overline{5^{3}} \\
&= \overline{5^{6}}^{343} \cdot \overline{5^{3}} \\
&\qquad \uparrow \longrightarrow = \bar{1} \\
&= \bar{1} \cdot \overline{5^{3}} \\
&= \overline{25} \cdot \bar{5} \\
&= \bar{4} \cdot \bar{5} \\
&= \bar{6} \qquad \text{Ok !}
\end{aligned}$$

L'esercizio sulla cometa è tratto da D.M.Burton und H. Dalkowski - *Handbuch der elementaren Zahlentheorie*

ESERCITAZIONE N.8

26 novembre 2007

- Il teorema di Eulero
- Gli elementi invertibili di Z_n
- Equazioni in Z_n
- Numeri complessi: la forma algebrica

Rosalba Barattero

ESERCIZIO 1 .

Il teorema di Eulero - L'inverso di un elemento in Z_n

a) In Z_{45} determinare r, $0 \le r < 45$, t.c. $\bar{r} = \bar{7}^{313}$.

b) Stabilire perché $\bar{7}^{313}$ è invertibile in Z_{45} e determinarne l'inverso.

a) Il piccolo teorema di Fermat non ci aiuta in questo caso perché non siamo in Z_p, con p primo. Ma c'è la seguente generalizzazione:

TEOREMA DI EULERO:
Se a ed n sono due interi coprimi (primi fra loro) allora si ha $\bar{a}^{\varphi(n)} = \bar{1}$ ***in*** Z_n ***, dove la funzione di Eulero*** $\varphi(n)$ ***indica il numero degli interi positivi, minori di n, che sono primi con n.***

Nel nostro caso n=45, a=7, M.C.D.(7,45)=1, quindi si può applicare il teorema di Eulero. Occorre trovare $\varphi(45)$, ossia il numero di interi positivi x<45, che sono primi con 45.
1,2,4,7,8, …
Meglio disporre di qualche regola per trovare $\varphi(45)$.

- $\varphi(p) = p-1$ con p primo (in questo caso il teor. di Eulero si riduce al piccolo teorema di Fermat !)
- $\varphi(p^s) = p^s - p^{s-1}$ con p primo
- se $n = a \cdot b$, con a,b coprimi, allora $\varphi(n) = \varphi(a) \cdot \varphi(b)$
- se si decompone n in fattori primi $\varphi(n)$ è determinato con le 2 proprietà precedenti …

$45 = 5\cdot 9 = 5\cdot 3^2$, 5 e 3^2 sono coprimi, allora risulta $\varphi(45) = \varphi(5)\cdot\varphi(3^2)$. Ma 5 è primo, quindi $\varphi(5) = 5-1=4$, anche 3 è primo, quindi $\varphi(3^2)=3^2-3^1$, perciò $\varphi(9)=6$,e di conseguenza $\varphi(45)=\varphi(5)\cdot\varphi(9)= 4\cdot 6=24$.

Applichiamo il teorema di Eulero: $\bar{a}^{\varphi(n)} = \bar{1}$ in Z_n, perciò $\bar{7}^{\varphi(45)} = \bar{1}$ in Z_{45}, ossia $\bar{7}^{24} = \bar{1}$ in Z_{45} .

Ora calcoliamo $\bar{7}^{313}$, dividendo l'esponente per 24.

$$\bar{7}^{313} = \bar{7}^{24\cdot 13+1} = \left(\bar{7}^{24}\right)^{13}\cdot\bar{7} = \left(\bar{1}\right)^{13}\cdot\bar{7} = \bar{7}.$$

Quindi $\bar{7}^{313} = \bar{7} \Rightarrow$ r=7 risponde alla domanda a).

b) Ora c'è una proprietà che stabilisce quali sono gli elementi invertibili di Z_n .

In Z_n $\bar{a} \neq \bar{0}$ è invertibile $\Leftrightarrow$ M.C.D.(a,n)=1.

Nel nostro caso: M.C.D.(7,45)=1$\Rightarrow \bar{7}$ è invertibile in Z_{45} .
Allora si può trovare l'inverso moltiplicativo di $\bar{7}$, ossia (l'unico) $\bar{x} \in Z_{45}$ tale che $\bar{7}\cdot\bar{x} = \bar{1}$.

$\bar{7}\cdot\bar{x} = \bar{1}$ in $Z_{45} \Leftrightarrow \overline{7x} = \bar{1}$

$\Leftrightarrow 7x \equiv 1$ (due classi di eq.va coincidono $\Leftrightarrow$ i loro rappresentanti sono equivalenti, che in questo caso vuol dire congruenti)

$\Leftrightarrow$ 7x -1 è multiplo di 45 in Z (def. di congruenza)

$\Leftrightarrow \exists\, y \in Z$ t.c. 7x -1 = 45y

Dunque il problema si è ridotto alla risoluzione dell'equazione lineare 7x – 45y=1 in Z, più precisamente dobbiamo trovare una sua soluzione (a,b)$\in$ ZxZ (in pratica poi utilizzeremo solo la "a" trovata).

Sappiamo già che questa equazione ha soluzioni in Z perché M.C.D.(7,45)=1 .

Troviamo una soluzione intera,usando l'algoritmo euclideo:

$45 = 7\cdot 6+3 \longrightarrow 3 = 45 - 7\cdot 6$ ↑

$7 = 3\cdot 2+1 \longrightarrow 1 = 7 - 3\cdot 2$

$3 = 1\cdot 3$

Quindi $1 = 7 - 3\cdot 2$
$= 7 - (45-7\cdot 6)2$
$= 7 - 45\cdot 2+7\cdot 12$
$= 7\cdot 13 - 45\cdot 2$

Da $1 = 7\cdot 13-45\cdot 2$ passando alle classi modulo 45, ricaviamo

$\bar{1} = \overline{7\cdot 13} - \overline{45\cdot 2}$ in Z_{45}

$= \bar{7}\cdot\overline{13}$ ($\overline{45} = \bar{0}$ in Z_{45}) $\Rightarrow \quad \bar{x} = \overline{13}$ è l'inverso di $\bar{7}$.

ESERCIZIO 2.

Equazioni lineari in Z_n

a) Risolvere l'equazione $\overline{12}\cdot x=\overline{0}$ in Z_{13}
b) Risolvere l'equazione $\overline{12}\cdot x=\overline{0}$ in Z_{48}
c) Risolvere l'equazione $\overline{14}\cdot x=\overline{21}$ in Z_{77}.

a) E' un'eq.ne del tipo ax=b con i coefficienti in Z_n, di cui cerchiamo le soluzioni in Z_n, cioè gli $\overline{x}\in Z_{13}$ t.c. $\overline{12}\cdot\overline{x}=\overline{0}$.
Intanto notiamo che $\overline{x}=\overline{0}$ è soluzione. Ce ne sono altre?
La domanda ha senso perché sappiamo che negli Z_n possono esistere due elementi non nulli il cui prodotto è zero (si chiamano 0-divisori).

Considerando la stessa eq.ne ax=0 in R, con a ≠0 otterremmo l'unica soluzione x=0 dividendo per a , ossia moltiplicando ambo i membri per l'inverso a^{-1} di a.
Qua si può fare lo stesso procedimento con l'operazione di moltiplicazione tra classi, **purché esista l'inverso di** $\overline{12}$.

Si sa che in Z_n $\overline{a}\neq\overline{0}$ è invertibile $\Leftrightarrow$M.C.D.(a,n)=1.
Qui M.C.D.(12,13)=1, quindi $\overline{12}$ è invertibile, chiamiamo $\overline{12}^{-1}$ il suo inverso (è unico !). Risulta:

$$\overline{12}\cdot\overline{x}=\overline{0}\Leftrightarrow\overline{12}^{-1}(\overline{12}\cdot\overline{x})=\overline{12}^{-1}\cdot\overline{0}\Leftrightarrow(\overline{12}^{-1}\cdot\overline{12})\cdot\overline{x}=\overline{0}$$
$$\Leftrightarrow\overline{1}\cdot\overline{x}=\overline{0}$$
$$\Leftrightarrow\overline{x}=\overline{0}.$$ Quindi c'è solo la soluzione nulla $\overline{x}=\overline{0}$.

Lo studente S. osserva che qua abbiamo mostrato che in Z_n un elemento invertibile non può essere 0-divisore. Ciò è noto dalla teoria in cui si è visto che:
"ogni elemento non nullo di Z_n o è invertibile o è zero divisore (una delle due !)"

b) L'equazione è $\overline{12}\cdot x=\overline{0}$ in Z_{48} .
Notiamo che $\overline{0}$ è soluzione, ma non è l'unica, infatti anche $\overline{4}$ ($\overline{12}\cdot\overline{4}=\overline{48}=\overline{0}$) è soluzione.

Ciò che differenzia b) da a) è il fatto che qua M.C.D.(12,48) = 12 ≠ 1 e quindi $\overline{12}$ non è invertibile e di conseguenza secondo la nota precedente è 0-divisore

Ma se $\overline{4}$ è sol^ne allora sono soluzione anche tutti gli elementi del tipo $\overline{4k}$ con $k\in Z$, quindi :
$\overline{8}$($\overline{12}\cdot\overline{4}\cdot\overline{2}=\overline{48}\cdot\overline{2}=\overline{0}$), $\overline{12}$ ($\overline{12}\cdot\overline{4}\cdot\overline{3}=\overline{48}\cdot\overline{3}=\overline{0}$) e …
quante sono ?
Si intuisce che sono…12, ma vediamo la risposta generale

TEOREMA
In Z_n l'equazione $\overline{a}\cdot x=\overline{b}$, con $\overline{a}\neq\overline{0}$, ha soluzioni se e solo se d= M.C.D. (a,n) divide b.
E in tal caso ci sono d soluzioni distinte, esprimibili nella forma

$$\overline{x_0},\overline{x_0+c},\overline{x_0+2c},\ldots,\overline{x_0+(d-1)c}$$

dove c=$\frac{n}{d}$ e $\overline{x_0}$ è una soluzione dell'equazione.

Qui: n=48, a=12, b=0, $\overline{x_0}=\overline{0}$ (sol.^ne trovata prima)
Si ha M.C.D.(12,48)=12=d e 12 divide 48, quindi l'equazione data ha 12(=d) soluzioni:

$$\overline{0},\ \overline{0+4}=\overline{4},\overline{4\cdot2}=\overline{8},\overline{4\cdot3}=\overline{12},\overline{4\cdot4}=\overline{16},\overline{4\cdot5}=\overline{20},$$
$$\overline{4\cdot6}=\overline{24},\overline{4\cdot7}=\overline{28},\overline{4\cdot8}=\overline{32},\overline{4\cdot9}=\overline{36},\overline{4\cdot10}=\overline{40},$$
$$\overline{4\cdot11}=\overline{44}\ \text{ stop !}$$

Perché procedendo si ritorna alla prima soluzione scritta $\overline{0}$ ($\overline{4 \cdot 12} = \overline{48} = \overline{0}$) e così via ciclicamente.
Ogni soluzione è individuata dalla precedente con l'aggiunta di 4 sotto la barra !

c) Risolvere l'equazione $\overline{14} \cdot x = \overline{21}$ in Z_{77}

Come in b) M.C.D.(14,77)=7 che divide 21, quindi 7 soluzioni distinte.

Occorre trovare una soluzione $\overline{x_0}$, per semplicità di notazione la chiamiamo $\overline{x}$, e cerchiamo $x \in Z$ t.c. $\overline{14} \cdot \overline{x} = \overline{21}$.

Se non si trova 'a occhio', si passa in Z:
risolvere $\overline{14x} = \overline{21}$ in Z_{77} equivale a risolvere in Z l'equazione diofantea 14x-21=77y, che riscriviamo 14x-77y= 21.

Se anche a questo punto la soluzione non si vede 'a occhio', il metodo per trovare una soluzione intera è quello dell'algoritmo di Euclide, che applichiamo all'equazione data o a quella semplificata(*) per 7 (provare per esercizio questo caso, in cui si può lavorare con numeri un pochino più piccoli).

Lo studente F. osserva che semplificando l'equazione 14x-77y = 21 per 7 si trova l'equazione equivalente 2x-11y = 3, da cui è immediato vedere la soluzione (7,1) e concludere $\overline{x} = \overline{7}$.

$77 = 14 \cdot 5 + 7 \longrightarrow 7 = 77 - 14 \cdot 5$ *
$14 = 7 \cdot 2$

Abbiamo scritto 7 come combinazione lineare di 77 e 14, ma poiché ci serve la combinazione lineare per il 21, moltiplichiamo l'uguaglianza * per 3.
$7 \cdot 3 = 77 \cdot 3 - 14 \cdot 5 \cdot 3$ da cui
$21 = 77 \cdot 3 - 14 \cdot 15$.

Ci interessa x, il coefficiente di 14, che è –15 (attenti al segno !).
Così abbiamo trovato x=-15 in Z, da cui $\overline{x} = \overline{-15}$ in Z_{77}, ossia $\overline{x} = \overline{-15 + 77} = \overline{62}$.

Conclusione: $\overline{x} = \overline{62}$ è una sol.ne dell'eq.ne $\overline{14} \cdot x = \overline{21}$ in Z_{77}
Le 7 soluzioni distinte con la tecnica del teorema,sono:
$\overline{62}$,
$\overline{62+11} = \overline{73}$,
$\overline{73+11} = \overline{84} = \overline{77+7} = \overline{7}$,
$\overline{7+11} = \overline{18}$,
$\overline{18+11} = \overline{29}$,
$\overline{29+11} = \overline{40}$,
$\overline{40+11} = \overline{51}$.

(*) Alla domanda "Ci conviene sempre semplificare l'equazione diofantea ax+by=c in una equivalente previa riduzione a fattor comune dei coefficienti?" rispondo sì, se si vede il fattore (!) e sì, a meno che la domanda della ricerca delle soluzioni non sia preceduta dalla domanda di trovare M.C.D.(a,b) tramite l'algoritmo euclideo, poiché in tal caso si dispone già dei dati per scrivere l'identità di Bezout e quindi una soluzione particolare della diofantea.

ESERCIZIO 3 .

Calcoli in **C** con la forma algebrica

Esprimere nella forma a+ib i seguenti numeri complessi

a) (2-3i)(1+i)

b) $i^5 + (1+i)^{32}$

c) $\frac{1}{3-i}$

RICORDIAMO :

- i numeri complessi C estendono i numeri reali R ($R \subset C$)
- la loro rappresentazione algebrica è a+ib, con a , b numeri reali, i unità immaginaria t.c. $i^2=-1$
- le 4 operazioni si fanno con le consuete regole del calcolo algebrico

a) (2-3i)(1+i) = 2-3i+2i+3 = 5-i

b) $i^5 + (1+i)^{32}$ = ?

$i^5 = (i)\,(i^2)^2$ (proprietà delle potenze)

$= i\,(-1)^2$ ($i^4 = 1$ ⟵ da ricordare !)

$= i$

$(1+i)^{32} = ((1+i)^2)^{16} = (1-1+2i)^{16} = (2i)^{16} = 2^{16}\, i^{16} = 2^{16}\,(i^4)^4$

$= 2^{16}\,(1)^4$

$= 2^{16}$

$\Rightarrow i^5 + (1+i)^{32} = 2^{16} + i$

Siamo stati fortunati a poter procedere così !
Per convincersene controllare se è possibile calcolare $(1+i\sqrt{3})^{100}$ con semplici passaggi come sopra.
In generale le potenze in **C** si calcolano agevolmente passando alla forma trigonometrica con la formula di De Moivre,come vedremo.

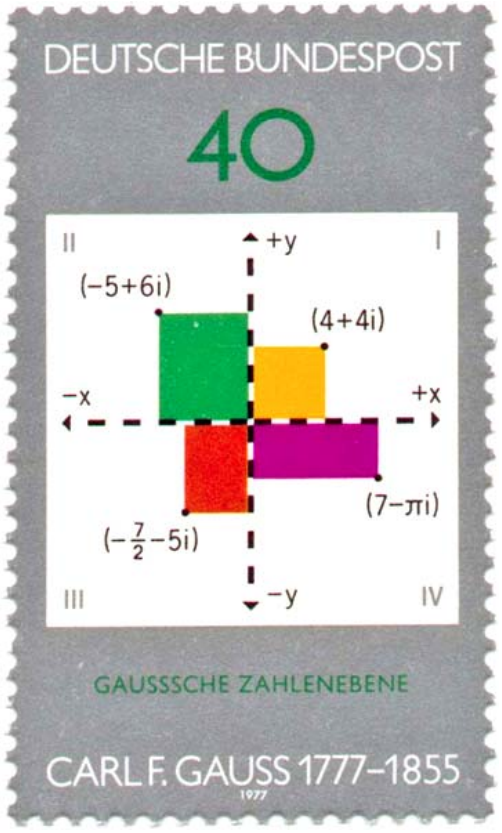
c) $\frac{1}{3-i} = \frac{(3+i)}{(3-i)(3+i)} = \frac{(3+i)}{10} = \frac{3}{10} + i\frac{1}{10}$

Si moltiplica numeratore e denominatore per il coniugato del denominatore

Se z= a+ib , si chiama coniugato di z il numero complesso $\bar{z}$ =a-ib.

Il prodotto $z \cdot \bar{z}$ è sempre un numero reale = a^2+b^2.

RAPPRESENTAZIONE DEI NUMERI COMPLESSI NEL PIANO DI ARGAND- GAUSS



200. esimo compleanno Di Gauss
Germania 1977

http://www.fh-friedberg.de/users/boergens/marken/beispiele/komplex.htm

z

ESERCITAZIONE N.9

4 dicembre 2007

- Calcoli nei numeri complessi:

  forma algebrica e trigonometrica
- Il piano di Argand-Gauss
- Formula di De Moivre
- Risoluzione in C delle equazioni

  $X^n-\alpha=0$

Rosalba Barattero

RAPPRESENTAZIONE TRIGONOMETRICA IN C

I numeri reali, si possono rappresentare geometricamente come punti di una retta. Anche i numeri complessi si possono rappresentare geometricamente, ma come punti del piano reale.

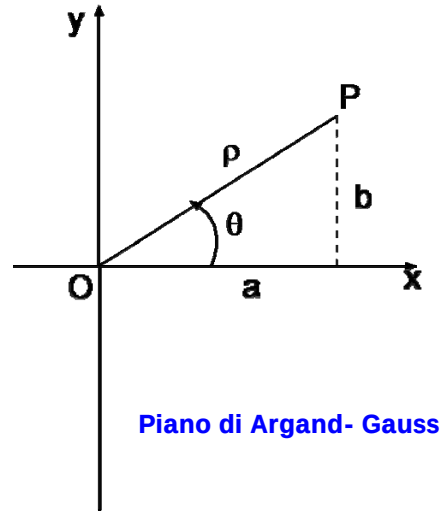
Si introduce nel piano reale un sistema $O_{x,y}$ di coordinate cartesiane ortogonali e si associa al numero complesso z=a+ib il punto P(a,b).

z=a+ib ⟷ coppia ordinata (a,b) di **R**x**R** ⟷ punto P(a,b)

ρ = distanza di P(a,b) dall'origine O
= $\sqrt{a^2+b^2}$
= modulo di z =|z|

θ = angolo formato in senso antiorario dalla semiretta positiva dell'asse x con la semiretta OP
argomento di z = Arg(z)
(∀z≠0) definito a meno di multipli di 2π, ossia
Arg(z) = θ+2kπ, k ∈ **Z**

Si suppone z≠0 poiché se z=0 l'argomento è indeterminato.



Piano di Argand- Gauss

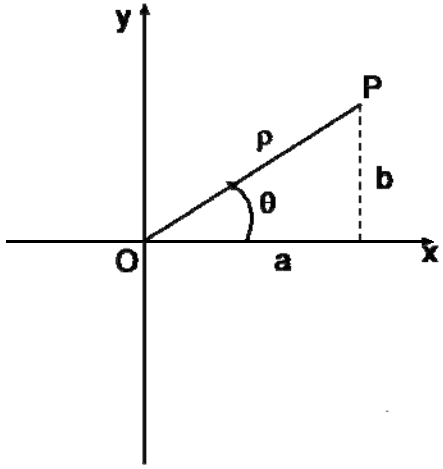
x asse reale (complessi con b=0)
y asse immaginario (complessi con a=0)

Dalle formule trigometriche per i triangoli rettangoli si ha :

$a = \rho \cos\theta$, $b = \rho \operatorname{sen}\theta$

e quindi

$z = \rho(\cos\theta + i \operatorname{sen}\theta)$
forma trigonometrica del numero complesso $z = a+ib$



Forma algebrica ⟶ Forma trigonometrica

$z=a+ib$ ⟶ $z = \rho(\cos\theta + i \operatorname{sen}\theta)$

Dato $z=a+ib$ $(z\neq 0)$ si calcolano ρ e θ

$$\begin{cases} \rho = \sqrt{a^2+b^2} \quad \text{(teorema di Pitagora)} \\ \vartheta = \text{l'angolo def. a meno di multipli di } 2\pi \text{ t.c.} \\ \cos\vartheta = \dfrac{a}{\sqrt{a^2+b^2}}, \ \operatorname{sen}\vartheta = \dfrac{b}{\sqrt{a^2+b^2}} \end{cases}$$

ESERCIZIO 1.

Calcoli in C con la forma trigonometrica

Disegnare nel piano di Argand-Gauss i seguenti numeri complessi e rappresentarli in forma trigonometrica:

a) 2i b) -3i c) -1 d) 1+i

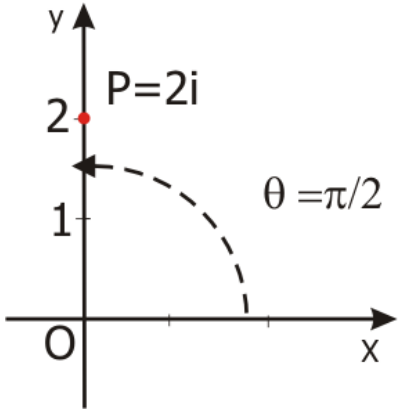
a)

$2i = 0+2i \longrightarrow P(0,2)$

ρ e θ si leggono qui dal disegno.

$\rho = d(P,O)=2$

$\theta = \frac{\pi}{2}$ (a meno di multipli di 2π).



Verifichiamo l'esattezza dei valori trovati per ρ e θ tramite le formule precedenti: $2i = a+ib$ con $a= 0$, $b = 2$

$$\Rightarrow \rho = \sqrt{a^2+b^2} = \sqrt{4} = 2$$

$$\cos\vartheta = \frac{a}{\sqrt{a^2+b^2}} = \frac{0}{2} = 0 \ , \quad \operatorname{sen}\vartheta = \frac{b}{\sqrt{a^2+b^2}} = \frac{2}{2} = 1$$

$$\Rightarrow \theta = \text{Arg}(z) = \frac{\pi}{2} + 2k\pi \ , \ k \in Z$$

Quindi la forma trigonometrica di z è :

$z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta) = 2\left(\cos\frac{\pi}{2} + i\,\mathrm{sen}\,\frac{\pi}{2}\right)$

scriviamo l'unico angolo θ, $0 \le \theta < 2\pi$

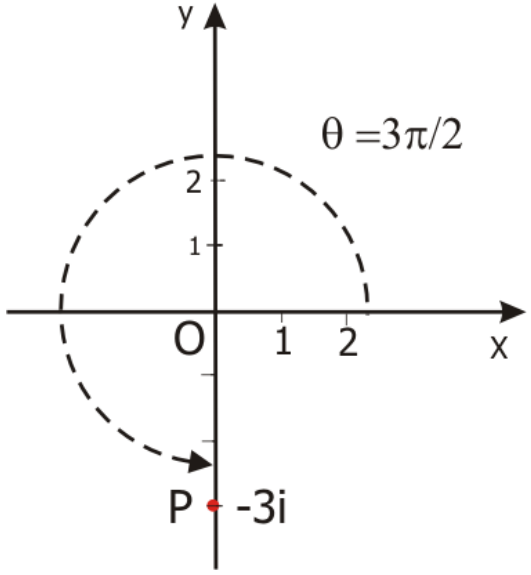
t.c. $\cos\theta = 0$ e $\mathrm{sen}\,\theta = 1$

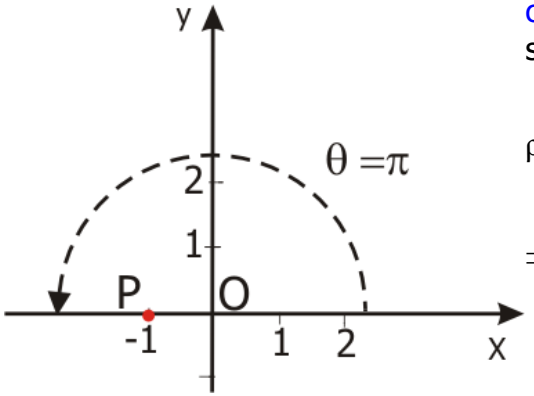
b) z=-3i : sta sull'asse immaginario negativo

$\rho = 3$, $\theta = \frac{3\pi}{2}$ (a meno di multipli di 2π)

$\Rightarrow z = 3\left(\cos\frac{3\pi}{2} + i\,\mathrm{sen}\,\frac{3\pi}{2}\right)$

(oppure $z = 3\left(\cos -\frac{\pi}{2} + i\,\mathrm{sen} -\frac{\pi}{2}\right)$)





c) z=-1
sta sull'asse reale negativo

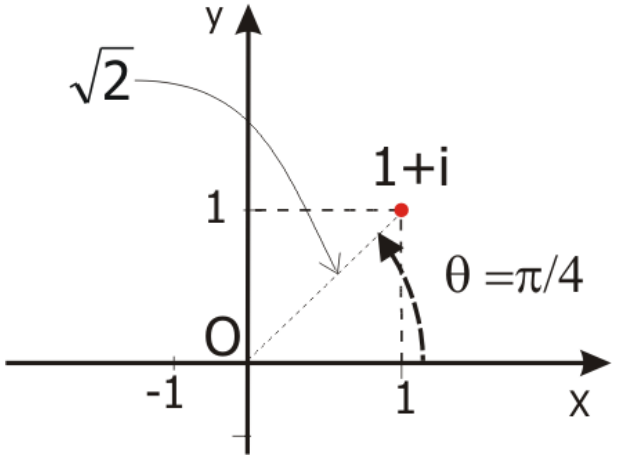
$\rho = 1$, $\theta = \pi$ (a meno di multipli di 2π)

$\Rightarrow z = 1(\cos\pi + i\,\mathrm{sen}\,\pi)$

d) $z = a + ib = 1 + i \longrightarrow P(1,1)$

dal disegno : $\theta = \pi/4$, $\rho = \sqrt{a^2 + b^2} = \sqrt{2}$

$\Rightarrow z = \sqrt{2}\left(\cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4}\right)$



MOLTIPLICAZIONE – DIVISIONE – POTENZE NELLA FORMA TRIGONOMETRICA

PRODOTTO

$z_1=\rho_1(\cos\theta_1 +i\,\mathrm{sen}\theta_1)$, $z_2=\rho_2(\cos\theta_2 +i\,\mathrm{sen}\theta_2)$, $z_1\neq 0, z_2\neq 0$

$\Rightarrow\ z_1 z_2 =\rho_1\rho_2\,(\cos(\theta_1+\theta_2) +i\,\mathrm{sen}(\theta_1+\theta_2))$

Il prodotto di due numeri complessi è il numero complesso avente per modulo il prodotto dei moduli e per argomento la somma degli argomenti

$$|z_1 z_2| = |z_1||z_2| \quad \& \quad \mathrm{Arg}(z_1 z_2)= \mathrm{Arg}(z_1)+ \mathrm{Arg}(z_2)$$

QUOTO

$$\frac{z_1}{z_2}=\frac{\rho_1(\cos\vartheta_1+isen\vartheta_1)}{\rho_2(\cos\vartheta_2+isen\vartheta_2)}=\frac{\rho_1}{\rho_2}(\cos(\vartheta_1-\vartheta_2)+isen(\vartheta_1-\vartheta_2))$$

Il quoto di due numeri complessi è il numero complesso avente per modulo il quoto dei moduli e per argomento la differenza degli argomenti.

$$\left|\frac{z_1}{z_2}\right|=\frac{|z_1|}{|z_2|} \quad \& \quad Arg\left(\frac{z_1}{z_2}\right)=Arg(z_1)-Arg(z_2)$$

POTENZA (FORMULA DI DE MOIVRE)

$z=\rho\,(\cos\theta +i\,\mathrm{sen}\theta) \quad \Rightarrow\ z^n=\rho^n\,(\cos(n\theta) +i\,\mathrm{sen}(n\theta))$

$(z\neq 0)$ PER OGNI $n\in Z$

La potenza di un numero complesso è il numero complesso avente per modulo la potenza del modulo e per argomento il prodotto dell'argomento per l'esponente.

$$|z^n|=|z|^n \ \&\ \mathrm{Arg}(z^n)=n\,\mathrm{Arg}(z)$$

ESERCIZIO 2.

Calcoli in C con la forma trigonometrica e l'algebrica

Determinare la parte reale Re(z) e la parte immaginaria Im(z) del numero complesso $z=\frac{(1+i)^{47}}{(1-i)^{50}}$

I° MODO

In ***questo caso particolare*** si può anche procedere così, tenendo conto che

$(1+i)^2 = (1+2i+i^2) = (1+2i-1) = 2i$ e

$(1-i)^2 = (1-2i+i^2) = (1-2i-1) = -2i$

Calcoliamo numeratore e denominatore

$$\begin{aligned}(1+i)^{47} &= ((1+i)^2)^{23}(1+i)\\ &= (2i)^{23}(1+i)\\ &= 2^{23}(i)^{23}(1+i)\\ &= 2^{23}(-i)(1+i) \qquad [\,i^4=1 \Rightarrow i^{23}=(i^4)^5\,i^3=i^3=-i\,]\\ &= 2^{23}(1-i)\end{aligned}$$

$$\begin{aligned}(1-i)^{50} &= ((1-i)^2)^{25}\\ &= (-2i)^{25}\\ &= (-2)^{25}(i)^{25}\\ &= -2^{25}i \qquad [i^4=1 \Rightarrow i^{25}=(i^4)^6\,i=i\,]\end{aligned}$$

Passiamo ora alla frazione

$$\frac{(1+i)^{47}}{(1-i)^{50}} = \frac{2^{23}(1-i)}{-2^{25}i} = \frac{1-i}{-2^2 i} = \frac{1-i}{-4\,i}$$

Ora si tratta di fare la divisione tra due numeri complessi scritti entrambi nella forma a+ib : la regola dice che si moltiplica numeratore e denominatore per il coniugato del denominatore , che nel nostro caso è 4i, qua si può procedere semplicemente moltiplicando solo per i, ma …seguiamo la regola):

$$\frac{1-i}{-4\,i} = \frac{(1-i)(4i)}{(-4i)(4i)}$$

$$= \frac{(4+4i)}{16}$$

$$= \frac{1}{4}+\frac{1}{4}i \quad \Rightarrow \text{Re}(z)= \tfrac{1}{4}\ ,\ \text{Im}(z) = \tfrac{1}{4}.$$

Questo modo è stato mostrato per l'interesse che ha sul calcolo algebrico nei complessi, ma si può fare uso della forma trigonometrica e procedere in modo alternativo così

II° MODO

Portiamo numeratore e denominatore in forma trigonometrica:
Iniziamo con la base del numeratore:

1+i : a=1,b=1 $\Rightarrow$ $\rho = \sqrt{a^2+b^2} = \sqrt{2}$,

$$\cos\vartheta = \frac{a}{\sqrt{a^2+b^2}} = \frac{1}{\sqrt{2}}\ ,\ sen\vartheta = \frac{b}{\sqrt{a^2+b^2}} = \frac{1}{\sqrt{2}} \Rightarrow \vartheta = \frac{\pi}{4}$$

$$\Rightarrow 1+i = \rho(\cos\vartheta + i sen\vartheta)$$

numeratore = $(1+i)^{47} = [(\sqrt{2})(\cos\frac{\pi}{4}+\text{isen}\frac{\pi}{4})]^{47}$

usiamo la formula di De Moivre per la potenza

$$= (\sqrt{2})^{47}(\cos\frac{47\pi}{4}+\text{isen}\frac{47\pi}{4})$$

riduciamo l'angolo modulo 2π(*): $\frac{47\pi}{4} = 12\pi - \frac{\pi}{4} \Rightarrow$ l'angolo è $-\frac{\pi}{4}$

$$= \sqrt{2^{47}}\ (\cos -\frac{\pi}{4}+\text{isen} -\frac{\pi}{4})$$

denominatore $(1-i)^{50} = [(\sqrt{2})(\cos -\frac{\pi}{4}+\text{isen} -\frac{\pi}{4})]^{50}$

usiamo la formula di De Moivre per la potenza

$$= \sqrt{2^{50}}(\cos -\frac{50\pi}{4}+\text{isen} -\frac{50\pi}{4})$$

ma $-\frac{50\pi}{4} = -12\pi - \frac{2\pi}{4}$ quindi l'angolo è $-\frac{2\pi}{4}$

$$= \sqrt{2^{50}}\ (\cos -\frac{2\pi}{4}+\text{isen} -\frac{2\pi}{4})$$

Passiamo ora alla frazione:

$$\frac{\sqrt{2^{47}}(\cos -\frac{\pi}{4}+\text{isen} -\frac{\pi}{4})}{\sqrt{2^{50}}(\cos -\frac{2\pi}{4}+\text{isen} -\frac{2\pi}{4})}$$ usiamo formula di De Moivre per il quoto

$$= \frac{1}{\sqrt{2^3}}[\cos(-\frac{\pi}{4}+\frac{2}{4}\pi)+\text{isen}(-\frac{\pi}{4}+\frac{2}{4}\pi)]$$

$$= \frac{1}{\sqrt{2^3}}[\cos(\frac{\pi}{4})+\text{isen}(\frac{\pi}{4})] = \frac{1}{\sqrt{2^3}}\ (\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}}) = \frac{1}{4}+\frac{1}{4}i$$

(*) Osservazione. Si possono anche lasciare gli argomenti al numeratore e denominatore così come sono, riducendo poi soltanto l'angolo $(\frac{47}{4}\pi+\frac{50}{4}\pi)$ che si ottiene dopo aver sottratto gli argomenti.

ESERCIZIO 3.

Risoluzione di equazioni in C

Determinare tutte le soluzioni in C delle seguenti equazioni e disegnarle nel piano di Argand-Gauss:

a) $Z^6=-1$

b) $Z^3 = 2-2i\sqrt{3}$

a) Nei reali l'equazione $Z^6=-1$ non ha soluzioni perché ogni numero reale non nullo elevato ad una potenza pari dà un numero positivo $a^6 = (a^3)^2 > 0$.
Nei complessi invece ogni equazione del tipo $Z^n = \alpha$, con $\alpha \neq 0$, ha esattamente tante soluzioni distinte quanto è il suo grado, ossia n. ♣

Per trovarle si fa così:

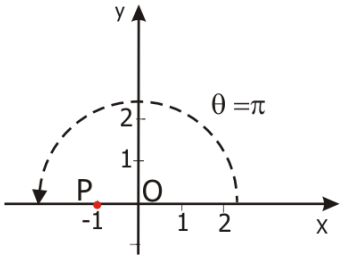
- si porta α in forma trigonometrica $\alpha = r(\cos\varphi + i\,\mathrm{sen}\varphi)$
- le n soluzioni distinte (dette radici n-esime di α) sono

$$z_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n} + i\,\mathrm{sen}\frac{\varphi+2k\pi}{n}\right)$$

attribuendo a k i valori 0,1,2,…,n-1.

♣ E' un caso particolare del TEOREMA FONDAMENTALE DELL'ALGEBRA provato da Gauss nella sua tesi di dottorato del 1799 per qualsiasi equazione a coefficienti in C.

$Z^6=-1$: portiamo -1 in forma trigonometrica, si era già visto nell'esercizio 1.



$z = 1(\cos\pi + i\,\mathrm{sen}\pi)$

$r=1$, $\varphi=\pi$

Le 6 (=n) radici distinte sono:

$$z_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n} + i\,\mathrm{sen}\frac{\varphi+2k\pi}{n}\right) \text{ , } k=0,1,2,3,4,5$$

$$\Rightarrow z_k = \cos\frac{\pi+2k\pi}{6} + i\,\mathrm{sen}\frac{\pi+2k\pi}{6} \text{ , } k=0,1,2,3,4,5$$

Da notare che le radici di $Z^n=\alpha$ hanno tutte lo stesso modulo ($=\sqrt[n]{r}$) e di conseguenza, nel piano di Argand- Gauss, sono disposte sulla *circonferenza* di centro l'origine e raggio $\sqrt[n]{r}$.
Inoltre due radici *'consecutive'* sono *'distanziate'* in senso angolare di un angolo pari a $\frac{2\pi}{n}$, quindi per determinare graficamente tutte le radici è sufficiente determinarne una per poter disegnare il *poligono regolare inscritto nella circonferenza di raggio* $\sqrt[n]{r}$, che ha come vertici le radici .

$k=0 \Rightarrow z_0 = \cos\frac{\pi}{6} + i\,\mathrm{sen}\frac{\pi}{6} = \sqrt{\frac{3}{2}} + \frac{1}{2}i$

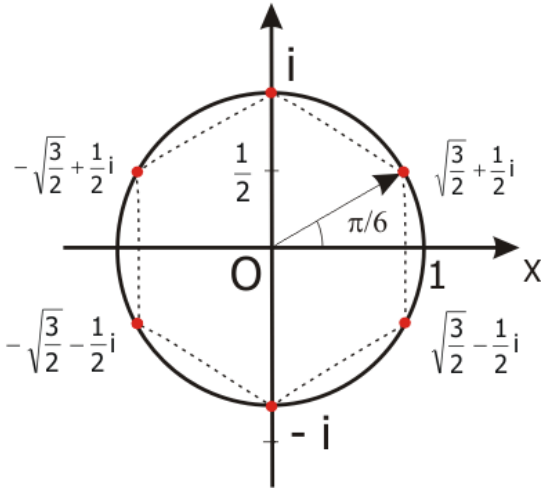
$k=1 \Rightarrow z_1 = \cos\frac{\pi}{2} + i\,\mathrm{sen}\frac{\pi}{2} = i$

$k=2 \Rightarrow z_2 = \cos\frac{5\pi}{6} + i\,\mathrm{sen}\frac{5\pi}{6} = -\sqrt{\frac{3}{2}} + \frac{1}{2}i$

$k=3 \Rightarrow z_3 = \cos\frac{7\pi}{6} + i\,\mathrm{sen}\frac{7\pi}{6} = -\sqrt{\frac{3}{2}} - \frac{1}{2}i$

$k=4 \Rightarrow z_4 = \cos\frac{3\pi}{2} + i\,\mathrm{sen}\frac{3\pi}{2} = -i$

$k=5 \Rightarrow z_5 = \cos\frac{11\pi}{6} + i\,\mathrm{sen}\frac{11\pi}{6} = \sqrt{\frac{3}{2}} - \frac{1}{2}i$



Le radici di $Z^n=\alpha$ sono i vertici di un poligono regolare di n lati inscritto nella crf. di raggio $\sqrt[n]{r}$.
Se $\alpha \in \mathbf{R}$ le radici sono a 2 a 2 complesse coniugate (simmetriche risp.asse x)

PROPRIETA'.
Una qualsiasi equazione, di grado dispari e a ***coefficienti reali*** ha almeno una radice reale !

Ciò dipende dal fatto che dopo che si sono accoppiate le radici complesse coniugate, ne resta almeno una che, dovendo essere la coniugata di se stessa, è necessariamente un numero reale !

- Ad es. dell'equazione $z^3-z^2+z-2=0$, che è a coefficienti reali, non abbiamo fornito una formula per trovarne le radici, ma essendo di grado dispari sappiamo che ha almeno una radice reale.*

- La proprietà aiuta anche a determinare le radici e la loro forma algebrica !
  Guardare il disegno: la simmetria risp. all'asse x traduce la proprietà: se c'è la radice a+ib , c'è anche la radice coniugata a-ib. (Mentre la sim metria risp. all'origine è legata al grado pari dell'equazione).

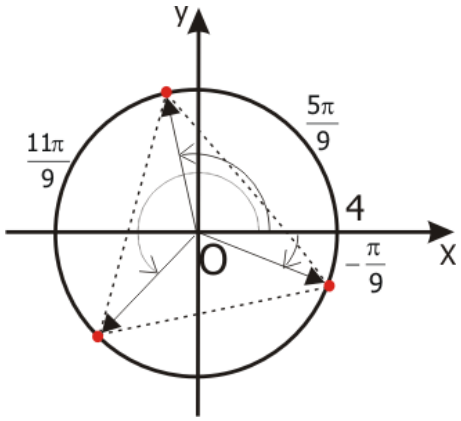
* L'analisi reale dà metodi approssimati per determinare tali radici e ne studia l'esistenza attraverso le informazioni date dalla derivata prima…

b) $Z^3 = 2-2i\sqrt{3}$

Questa equazione a differenza di quella studiata in a) è a coefficienti complessi e NON reali e perciò non vale più la regola che le sue radici sono complesse coniugate.

Ma è del tipo $Z^n=\alpha$, con $\alpha \in C$ e quindi le sue 3 radici costituiscono i vertici di un triangolo equilatero.

Con calcolo analogo ad a) si ricava:



$$z_0 = \cos -\frac{\pi}{9} + i\,\mathrm{sen}\,\frac{\pi}{9}$$

$$z_1 = \cos\frac{5\pi}{9} + i\,\mathrm{sen}\,\frac{5\pi}{9}$$

$$z_2 = \cos\frac{11\pi}{9} + i\,\mathrm{sen}\,\frac{11\pi}{9}$$

Parte II

Fogli di Esercizi
con suggerimento o risposta

Matematica Discreta a.a. 2007 - 2008

Foglio 1

ESERCIZI SULL' INDUZIONE

Usando il principio di induzione provare gli asserti da 1. a 9.

1. per ogni numero naturale n ≥1 vale l'uguaglianza: $1^3+2^3+3^3+\ldots+n^3=\left[\frac{n(n+1)}{2}\right]^2$
2. per ogni n≥1 il numero n^3+2n è divisibile per 3.
3. per ogni n≥1 vale l'uguaglianza: $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\ldots+\frac{n}{2^n}=2-\frac{n+2}{2^n}$
4. per ogni n n≥2 vale l'uguaglianza: $(1-\frac{1}{4})(1-\frac{1}{9})(1-\frac{1}{16})\cdots(1-\frac{1}{n^2})=\frac{1+n}{2n}$
5. per ogni n≥1 vale l'uguaglianza: $1+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$
6. per ogni n≥1 vale l'uguaglianza: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n(n+1)}=\frac{n}{n+1}$
7. per ogni n≥1 vale l'uguaglianza: $2+2^2+2^3+\ldots 2^n=2(2^n-1)$
8. per ogni n≥1 vale l'uguaglianza: $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)=\frac{n(n+1)(n+2)}{3}$
9. per ogni n≥1 vale l'uguaglianza: $1(1!)+2(2!)+3(3!)+\ldots+n(n!)=[(n+1)!]-1$
10. Individuare il valore della somma $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n\cdot(n+1)}$ utilizzando il seguente pattern

$$\frac{1}{1\cdot 2}=\frac{1}{2}$$
$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{2}{3}$$
$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{3}{4}$$
$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}=\frac{4}{5}$$

E verificare quindi la correttezza della risposta con il principio di induzione.

RISPOSTE

1. **Base dell'induzione:** La proprietà è *vera per n=1*. Sostituiamo 1 ad n:

$1^3=\left[\frac{1(1+1)}{2}\right]^2$ vera !

Passo dell'induzione: Se la proprietà (*) è vera per un generico n≥1 allora è vera anche per il successivo n+1.

Ipotesi induttiva: la proprietà è vera per n ,cioè $1^3+2^3+3^3+\ldots+n^3=\left[\frac{n(n+1)}{2}\right]^2$.

Tesi : La proprietà è vera per n+1, cioè (mettendo n+1 al posto di n)

$$1^3+2^3+3^3+\ldots+n^3+(n+1)^3=\left[\frac{(n+1)((n+1)+1)}{2}\right]^2$$
$$=\left[\frac{(n+1)(n+2)}{2}\right]^2$$

Scriviamo il membro di sinistra dell'uguaglianza della tesi:

$1^3+2^3+3^3+\ldots+n^3+(n+1)^3=$ **?**

$$[\text{ per l'ipotesi induttiva}]=\left[\frac{n(n+1)}{2}\right]^2+(n+1)^3$$
$$=\frac{n^2(n+1)^2+4(n+1)^3}{4}$$
$$=\frac{(n+1)^2(n^2+4(n+1))}{4}$$
$$=\frac{(n+1)^2(n+2)^2}{4}$$

abbiamo ottenuto esattamente il membro di destra della tesi. Ok!

2. Per n=1 ...è vero. Poi: $(n+1)^3+2(n+1)=(n^3+2n)+3n(n+1)+3$. Ora si usa l'ipotesi induttiva per cui $n^3+2n=3h$ con $h\in\mathbb{N}$...e si conclude:$(n+1)^3+2(n+1)$ multiplo di 3.
3. Per n=1 è vero. Poi per l'ipotesi induttiva si ha:

$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\ldots\frac{n}{2^n}+\frac{n+1}{2^{n+1}}=2-\frac{n+2}{2^n}+\frac{n+1}{2^{n+1}}=\ldots\ldots=2-\left(\frac{n+3}{2^{n+1}}\right)$. c.v.d.

4. Si riscrive così $(1-\frac{1}{2^2})(1-\frac{1}{3^2})(1-\frac{1}{4^2})\cdots(1-\frac{1}{n^2})=\frac{1+n}{2n}$. Per n=2 si ha

$1-\frac{1}{4}=\frac{1+2}{4}$: vero.

Poi usando l'ipotesi induttiva si ha:

$(1-\frac{1}{2^2})(1-\frac{1}{3^2})(1-\frac{1}{4^2})\cdots(1-\frac{1}{n^2})(1-\frac{1}{(n+1)^2}) = (\frac{1+n}{2n})(1-\frac{1}{(n+1)^2}) = \ldots\ldots = \frac{n+2}{2(n+1)}$.

5. Base induzione:...vera. Passo:per l'ipotesi induttiva si ha:

$1+2^2+3^2+\ldots+n^2+(n+1)^2 = \frac{n(n+1)(2n+1)}{6}+(n+1)^2 = \ldots$

$= \frac{(n+1)(2n^2+7n+6)}{6}$ che coincide con $\frac{(n+1)(n+2)(2n+3)}{6}$ c.v.d.

6. Per n=1 ... ok ! Poi si usa l'ipotesi induttiva:

$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)} = \frac{n}{n+1}+\frac{1}{(n+1)(n+2)} =$

$= \ldots = \ldots \frac{n+1}{n+2}$ c.v.d.

7. Per n=1 si ha : $2^1=2(2^1-1)$ ok ! Poi usando l'ipotesi induttiva

$2^1+2^2+2^3+\ldots+2^n+2^{n+1} = 2(2^n-1)+2^{n+1}$, che grazie alle proprietà delle potenze risulta $= 2(2^n-1)+2\cdot 2^n = 2(\ldots\ldots) = \ldots = 2(2^{n+1}-1)$ c.v.d.

8. Analogo ai precedenti: la tesi è $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)+(n+1)(n+2) = \frac{(n+1)(n+2)(n+3)}{3}$.

9. Base induzione:...vera. Passo:Si parte da $1(1!)+2(2!)+3(3!)+\ldots+n(n!)+(n+1)[(n+1)!]$ che,per l'ipotesi induttiva è uguale a $[(n+1)!]-1+(n+1)[(n+1)!]$. Si raccoglie e si ricava $[(n+1)!](1+n+1)-1$ ossia $[(n+2)!]-1$. c.v.d.

10. La risposta 'spontanea' è : $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$. Base induzione

(per n=1) è $\frac{1}{1\cdot 2} = \frac{1}{1+1}$: vera.

Passo induttivo: si parte da $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{(n+1)\cdot(n+2)}$ che per l'ipotesi induttiva

è uguale a $\frac{n}{n+1}+\frac{1}{(n+1)(n+2)}$, che con un paio di passaggi risulta coincidere con $\frac{n+1}{n+2}$

c.v.d.

Matematica Discreta a.a. 2007 - 2008

Foglio 2

ESERCIZI SULLE FUNZIONI

Es. 1 Sia $f : \mathbf{R}^2 \to \mathbf{R}^2$ la funzione definita da $f((x, y)) = (x + 2y,\ y + 1)$.
a) Provare che f è iniettiva e surgettiva.
b) Come è definita la funzione inversa f^{-1}?
c) Calcolare $f \circ f((1, 1))$.

Es. 2 Sia $f : \mathbf{Z} \to \mathbf{Z} \times \mathbf{N}$ la funzione data da $f(x) = (-2x + 3, x^2)$.
a) Stabilire se f è iniettiva e/o surgettiva.
b) Se $g : \mathbf{Z} \times \mathbf{N} \to \mathbf{Z}$ è la funzione definita da $g((a, b)) = a - 6b$, come sono definite le due funzioni $g \circ f$ e $f \circ g$?
c) Stabilire se l'insieme $\{x \in \mathbf{Z} \mid g \circ f(x) = x\}$ è non vuoto.

Es. 3 Sia $f : \mathbf{Z}^2 \to \mathbf{N}$ la funzione data da $f((x, y)) = |3x + y|$.
a) Stabilire se f è invertibile.
b) Sia $A = f^{-1}(10)$. Determinare quanti e quali sono gli elementi di $A \cap \mathbf{N}^2$.

Es. 4 Sia $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ la funzione data da $f((x, y)) = 2x + y^2$.
Stabilire se f è iniettiva e/o surgettiva.

Dopo avere svolto questi esercizi (tratti da compiti di esame antecedenti l' a.a. 2006/2007 - Corso di Matematica Discreta - Prof. G. Niesi) prendere visione delle 4 domande poste dagli studenti dello scorso anno e la relativa risposta. http://www.dima.unige.it/~baratter/funzioni_bottarisposta.pdf

RISPOSTE

1. a) Da $\begin{cases} x + 2y = a \\ y + 1 = b \end{cases}$ si ricava l'unica soluzione $\begin{cases} x = a - 2b + 2 \\ y = b - 1 \end{cases}$ che prova l'invertibilità di f e di conseguenza la sua bigettività.
   b) Da a) l'inversa è $f^{-1}: R^2 \to R^2$ definita da $f^{-1}(a,b)=(a-2b+2,b-1)$.
   c) $f \circ f((1,1)) = f(3,2) = (7,3)$

2. a) Iniettività : $f(x)=f(y) \Rightarrow (-2x+3,x^2)=(-2y+3,y^2) \Rightarrow -2x+3=-2y+3$ e $x^2=y^2 \Rightarrow x=y$
   $\Rightarrow$ f è iniettiva.
   f non è surgettiva: la controimmagine di (0,0) è $\varnothing$ perché da $(-2x+3,x^2)=(0,0)$ si ricava $-2x+3=0$ e $x^2=0$ e queste due equazioni non hanno alcuna soluzione comune.
   b) $f \circ g : ZxN \to ZxN$ è definita da $f \circ g\ (a,b) = \ldots (-2a+12b+3,(a-6b)^2)$, $g \circ f : Z \to Z$ è definita da $g \circ f\ (x) = \ldots = -2x+3-6x^2$.
   c) $g \circ f\ (x)=x \Leftrightarrow -2x+3-6x^2 = x \Leftrightarrow 2x^2+x-1=0$ e questa equazione ha la soluzione intera x=-1 , quindi l'insieme richiesto non è vuoto.

3. a) $(1,0) \neq (0,3)$ e $f((1,0))=f((0,3))=3 \Rightarrow$ f non è iniettiva $\Rightarrow$ f non è bigettiva $\Rightarrow$ f non è invertibile
   b) $A \cap N^2 = \{(0,10), (1,7), (2,4), (3,1)\}$ ed ha 4 elementi .

4. $f((0,2))=f((2,0))=4 \Rightarrow$ f non è iniettiva.
   Sia $n \in Z$ (codominio) distinguiamo due casi:
   - n = 2k (= pari) $\Rightarrow f((k,0)) = 2k = n$
   - n = k+1 (=dispari) $\Rightarrow f((k,1)) = 2k+1 = n$

   e quindi f è surgettiva.

Matematica Discreta a.a. 2007 - 2008

Foglio 3

ESERCIZI SULLE RELAZIONI D'EQUIVALENZA

1. Si consideri in Z la relazione $x \sim y \Leftrightarrow x^2+x=y^2+y$.
   a) Verificare che $\sim$ è una relazione d'equivalenza
   b) E' vero che $0 \sim -1$?
   c) Determinare le classi di equivalenza di 0, -2 e 7.
   d) E' vero che le classi di equivalenza sono costituite tutte da due elementi ?

2. Sia $\sim$ la relazione d'equivalenza in N^2 data da $(a,b) \sim (c,d) \Leftrightarrow a^2+b=c^2+d$.
   Dire quanti e quali sono gli elementi della classe di equivalenza di (3,1).

3. Sia $\sim$ la corrispondenza in Z^2 definita da $(a,b) \sim (c,d) \Leftrightarrow 2a-3b=2c-3d$
   a) Provare che $\sim$ è una relazione d'equivalenza
   b) Determinare tre elementi distinti di Z^2 equivalenti a (1,-1).

4. Sia $\sim$ la seguente corrispondenza in R
   $x \sim y \Leftrightarrow x^2-y^2 \in Z$.
   Stabilire se è una relazione d'equivalenza.

5. Sia $\sim$ la corrispondenza in Z^2 definita da $(a,b) \sim (c,d) \Leftrightarrow a^2 = c^2$.
   a) Verificare che $\sim$ è una relazione d'equivalenza.
   b) Determinare 3 elementi in $\overline{(2,1)}$

Oltre a questi esercizi (tratti da compiti d'esame antecedenti a.a. 2006/2007) sono interessanti le domande poste dagli studenti dello scorso anno e le relative risposte sulle relazioni d'equivalenza e sul calcolo combinatorio:
http://www.dima.unige.it/~baratter/comb-rel_bottarisp.pdf

RISPOSTE

1. a) Si può fare la verifica diretta che valgono le tre proprietà riflessiva, simmetrica e transitiva, o seguire in questo caso il metodo seguente:
   La relazione di equivalenza in Z associata alla funzione $f:Z \to Z$ definita da $f(t)=t^2+t$ è la seguente: $x \mathcal{R}_f y \Leftrightarrow f(x)=f(y)$.
   Risulta: $x \mathcal{R}_f y \Leftrightarrow x^2+x = y^2+y$. Allora $\sim$ coincide con $\mathcal{R}_f$, ed è quindi una relazione d'equivalenza.
   b) $0 \sim -1$ perché $0^2+0 = (-1)^2+(-1)$
   c) $\overline{0} = \{x \in Z \mid x \sim 0\} = \{x \in Z \mid x^2+x=0\} = \{0, -1\}$. Allo stesso modo si trova $\overline{-2} = \{1, -2\}$ e $\overline{7} = \{7, -8\}$.
   d) Sì, si può vedere che, per ogni $n \in Z$, $\overline{n} = \{n, -1-n\}$.
   Si può anche osservare che il discriminante dell'equazione $x^2+x=n^2+n$ (nell'incognita x) vale $1+4(n^2+n)$ e in Z è positivo, perché $n^2+n \geq 0$ in Z, quindi ... in R ci sono 2 radici reali distinte. La loro somma vale -1, una delle radici è n ... quindi...

2. La classe d'equivalenza di (3,1) è $\overline{(3,1)} = \{(x,y) \in \mathbb{N}^2 \mid (x,y) \sim (3,1)\} = \{(x,y) \in \mathbb{N}^2 \mid x^2+y=10\} = \{(0,10),(1,9),(2,6),(3,1)\}$, ed ha 4 elementi.

3. a) E' sufficiente verificare che $\sim$ coincide con la relazione d'equivalenza $\mathcal{R}_f$ associata alla funzione $f: Z^2 \to Z$ tale che $f((x,y))=2x-3y$.
   b) $(x,y) \sim (1,-1) \Leftrightarrow 2x-3y = 2(1)-3(-1) = 5$. Quindi tre elementi equivalenti a (1,-1) sono ad esempio: (1,-1),(-5,-5), (10,5).

4. Riflessiva: occorre verificare se vale $x \sim x$ per ogni $x \in R$. Per definizione $x \sim x$ equivale a $x^2-x^2 \in Z$, ossia $0 \in Z$, che è vera, quindi $x \sim x$ per ogni $x \in R$.
   Simmetrica: occorre verificare se è vero che $x \sim y \Rightarrow y \sim x \ \forall \ x,y \in R$. Si ha : $x \sim y \Leftrightarrow x^2-y^2 \in Z \Leftrightarrow y^2-x^2 \in Z$ (perché ...) $\Leftrightarrow y \sim x$. Quindi $\sim$ è simmetrica.
   Transitiva: ... $x \sim y$, $y \sim z \Rightarrow x \sim z$. Da $x^2-y^2 \in Z$ e $y^2-z^2 \in Z$ ... segue $x^2-z^2 \in Z$ e quindi $x \sim z$. Allora $\sim$ è transitiva.

5. a) $(a,b) \sim (a,b) \ \forall \ (a,b) \in Z^2$: vera perché $a^2 = a^2$. Per la simmetrica: $(a,b) \sim (c,d) \Leftrightarrow a^2 = c^2 \Leftrightarrow c^2 = a^2 \Leftrightarrow (c,d) \sim (a,b)$. Quindi la simmetrica è vera. Analoga la prova della transitività ...
   b) $(a,b) \sim (2,1) \Leftrightarrow a^2=4$. Quindi tre elementi cercati sono ad es. (2,1),(-2,1),(2,0).

Matematica Discreta a.a. 2007 - 2008

Foglio 4

ESERCIZI SULLA DIVISIONE, L'ALGORITMO EUCLIDEO E LE EQUAZIONI LINEARI IN Z

1. Determinare quoziente e resto delle seguenti divisioni

   1: -7 ; -2:-7; 61:-7.

2. Sia $A=\{n\in\mathbb{N} \mid 1\le n\le 1000\}$.

   a) Quanti sono gli elementi di A multipli di 50 ?

   b) Quanti sono gli elementi di A multipli di 12 ?

3. Si consideri a^2, con $a\in\mathbb{Z}$. Provare che il resto della divisione $a^2 : 4$ è 0, oppure 1.
   (Suggerimento: distinguere i due casi: a=2s (pari), a=2s+1 (dispari)).

4. In $\mathbb{Z}\times\mathbb{Z}$ sia ~ la corrispondenza $(a,b)\sim(c,d) \Leftrightarrow 2 \mid a+b+c+d$ (2 divide a+b+c+d).
   Stabilire se ~ è relazione d'equivalenza.

5. Calcolare il M.C.D. tra le seguenti coppie di interi e scrivere la corrispondente identità di Bezout

   a) (48, 276),

   b) (3054, 162)

6. Quali delle seguenti equazioni lineari non hanno soluzioni intere?

   a) 6x+51y=44

   b) 33x-14y=21

   c) -93x+105y=-24.

7. Determinare tutte le soluzioni intere delle seguenti equazioni lineari:

   a) 33x-14y=21

   b) 24x+138y=18

   c) 2x-5y=1

   d) 6x-15y=12.

8. Determinare tutte le soluzioni intere positive delle equazioni lineari dell'esercizio 7.

9. Determinare tutti i divisori primi di 50! (50 fattoriale).

10. **Eulero 1770.** Dividere 100 in due addendi, di cui uno sia divisibile per 7 e l'altro per 11.

RISPOSTE

1. q=0,r=1 ; q=1,r=5 ; q=-8,r=5

2.a) 20 perché 20·50 = 1000

   b) 83 perché 1000= 83·12+4

3. $a^2=(2s)^2=4s^2$ è multiplo di 4, quindi resto 0, $a^2=(2s+1)^2=\ldots = 4(\ldots)+1$, quindi resto 1.

4. (a,b)~(a,b) è vero perché a+b+a+b= 2(a+b). La simmetrica è vera perché...Per la transitiva:
   Da (a,b) ~(c,d) e (c,d)~(e,f) si ricava che : a+b+c+d=2h e c+d+e+f=2k, sottraendo queste due uguaglianze e ... si ricava a+b+e+f= 2(h-k), dunque 2| a+b+c+d.

5. a) 12=48(6)+276(-1)

   b) 6=3054(-7)+162(132).

6. Solo a) perché M.C.D.(6,51)=3 che non divide 44.

7. a) x=63+14t, y=147+33t al variare di t in Z

   b) Si può semplificare per 6 e lavorare sull'equazione equivalente 4x+23y=3, le cui soluzioni intere sono x=18+23t, y=-3-4t al variare di t in Z.

   c) x=-2+5t,y=-1+2t al variare di t in Z.

   d) x=-8+5t,y=-4+2t al variare di t in Z.

8. a) Il parametro t deve soddisfare entrambe le condizioni 63+14t>0, 147+33t>0.
   Entrambe conducono alla condizione t≥-4. Quindi l'equazione data ha soluzioni intere positive x=63+14t, y=147+33t, per t≥-4.

   b) Non esistono soluzioni intere positive.

   c) Per t≥1.

   d) Per t≥-1.

9. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

10. Dall'equazione 7x+11y=100 si ricava x=8, y=4, da cui gli addendi 56 e 44.

Matematica Discreta a.a. 2007 - 2008

Foglio 5

ESERCIZI SULL'ARITMETICA MODULARE

1. Utilizzando il piccolo teorema di Fermat calcolare il resto della divisione di 5^{38} per 11.
2. Usare il piccolo teorema di Fermat per provare che
   a) 17 divide m= 1+ 11^{104}
   b) 13 divide il numero N= 1+11^{12n+6} per ogni n≥0.
3. Per ogni n∈{2,5,13,21} stabilire se l'equazione $\overline{12}\cdot x=\overline{7}$ ha soluzioni in Z_n e, in caso affermativo, determinarle.
4. Quanti sono gli elementi invertibili di Z_{72} ? E quanti sono gli 0-divisori di Z_{72} ?
5. Quali sono le due ultime cifre di $\overline{2006}^{1188}$?
- 6. Quanti sono gli x interi, 1≤x≤ 1000, tali che $\overline{6}\cdot\overline{x}=\overline{23}$ in Z_{13} ?
- 7. Sia N il numero naturale la cui rappresentazione decimale è $a_n..\ a_2a_1a_0$ con $0\le a_i\le 9$, i =0,..n (ossia $N=10^n\cdot a_n+10^{n-1}\cdot a_{n-1}+...+10^2\cdot a_2+10^1\cdot a_1+10^0\cdot a_0$). Provare che 6 divide N se e solo se 6 divide il numero M= 4 a_n +4 a_{n-1} +...4a_1+a_0 .
- 8. Sia N un numero naturale con s cifre (nella sua rappresentazione decimale), s≥2. Determinare quali sono i possibili numeri formati dalle due ultime cifre di N nel caso in cui N sia divisibile per 25.
9. Provare che in Z_8 risulta $\overline{7}^n=\overline{1}$ se n è pari e $\overline{7}^n=\overline{7}$ se n è dispari .
10. Si consideri la funzione f:Z→Z_{10} definita da f(x)= $\overline{x}$: stabilire se f è iniettiva, surgettiva.
- 11. Determinare tutti gli n∈ℕ tali che $\overline{4}\cdot\overline{7}=\overline{2}^4$ in Z_n .
- 12. Provare facendo uso della teoria della congruenza il seguente fatto: per ogni n≥1 il numero n^3+2n è divisibile per 3.
13. Calcolare $\overline{a}^{-18}$ per ogni $\overline{a}\in Z_{19}$.
- 14. Provare che il quadrato di ogni intero dispari è congruo a 1 modulo 8.
15. Determinare esplicitamente l'insieme delle potenze di esponente r ≥0 della classe di 2 in Z_{13} , Z_{14} , Z_{15} , Z_{16} .

N.B. Gli esercizi contrassegnati con • sono facoltativi.

RISPOSTE

1. 4.
2. a) $\overline{11}^{16\cdot 6+8}=...=\overline{-1}$
   b) $\overline{11}^{12\cdot n+6}=...=\overline{-1}$
3. In Z_2 $\overline{12}\cdot x=\overline{7}$ equivale a ... : nessuna soluzione. In Z_5 unica soluzione $\overline{x}=\overline{1}$.
   In Z_{13} unica soluzione $\overline{x}=\overline{6}$; in Z_{21} nessuna soluzione.
4. Per il teorema di Eulero φ(72) = φ(3^2) φ(2^3) = ... = 24, quindi 24 elementi invertibili.
   E allora ci sono 71-24 = 47 0-divisori (lo zero si esclude).
5. In Z_{100} si ha $\overline{2006}^{1188}=\overline{6}^{1188}$. Calcolando $\overline{6}^2=\overline{36}$, $\overline{6}^3=...\overline{6}$, ... si trova $\overline{6}^{1188}=\overline{36}$.
   Ultime due cifre: 36.
6. $\overline{6}\cdot\overline{x}=\overline{23}\Leftrightarrow\overline{6}\cdot\overline{x}=\overline{10}$ in Z_{13} ha la soluzione $\overline{x}=\overline{6}$, ma $\overline{6}$ = {6+13k|k∈Z}, 1000-6 = ... , quindi il numero di interi richiesti è 77.
7. Procedere come per il criterio di divisibilità per 4.
8. 0,25,50,75.
9. $\overline{7}^{2k}=\left(\overline{7}^2\right)^k=...=\overline{1}$; $\overline{7}^{2k+1}=\overline{7}^{2k}\cdot\overline{7}=\overline{7}$.
10. f è surgettiva, ma non è iniettiva, ad esempio 10≠0 ma f(10)=f(0)= $\overline{0}$.
11. $\overline{28}=\overline{16}...\Rightarrow\overline{12}=\overline{0}$ che in Z_n vale se n divide 12, quindi n= 2,3,4,6.
12. $\overline{n^2}=\overline{1}$ in $Z_3-\{\overline{0}\}$ quindi $\overline{n^3+2n}=...=\overline{0}$.
13. $\overline{a}^{-18}=\overline{0}$ se $\overline{a}=\overline{0}$, altrimenti per il piccolo teorema di Fermat $\overline{a}^{-18}=\overline{1}$.
14. Sia a=2k+1 (k∈Z) un intero dispari. Il quadrato è $a^2=4k^2+4k+1$, quindi $a^2-1=4k(k+1)$. Siccome uno dei due numeri k, k+1 è pari, ne segue che a^2-1= 8 h (h∈Z) e quindi a^2 è congruo a 1 modulo 8.
15. L'insieme delle potenze di $\overline{2}$ in Z_{13} è Z_{13} -{$\overline{0}$}; in Z_{14} e Z_{15} è {$\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{8}$}; in Z_{16} è {$\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{8}$}.

Matematica Discreta a.a. 2007 - 2008

Foglio 6

ESERCIZI SUI NUMERI COMPLESSI

1. Determinare Re(z) e Im(z) dei seguenti numeri complessi:
   a) $z=\frac{-1+4i}{-1+2i}$ b) $z=\left(\cos\frac{2\pi}{3}+i\,sen\frac{2\pi}{3}\right)^4$
2. Determinare modulo ed argomento dei seguenti numeri complessi:
   a) $z=\frac{-1-i}{2-2i}$ b) $z=(1+i)^9$ c) $z=\frac{(1+i)^4}{(3-3i)^3}$
3. Sia $z\in\mathbf{C}$ tale che $|z|=3$ e $Arg(z) = -81\pi$. Determinare z in forma algebrica.
4. Siano $z_1=-\sqrt{3}+i$, $z_2=1-i$. Determinare
   a) $|z_1+z_2|$, $|z_1 z_2|$, $\left|\frac{z_1}{z_2}\right|$.
   b) $Arg(i z_1)$, $Arg\left(\frac{z_1}{z_2}\right)$, $Arg(3z_2)$
   c) Disegnare nel piano di Argand-Gauss $z_1, z_2, \overline{z_1}, \overline{z_2}$.
5. Scrivere in forma trigonometrica i seguenti numeri complessi:
   a) -13 b) $i\sqrt{2}$ c) $4-4\sqrt{3}i$.
6. Scrivere $\left(\frac{1+i\sqrt{3}}{1+i}\right)^8$ in forma algebrica.
7. Calcolare $i^5+i^6+i^7+\ldots.+i^{43}+i^{44}$.
8. Esercizio 7.123, pag. 90 , dispense di Niesi

* E' utile guardare le 3 domande-risposte
  http://www.dima.unige.it/~baratter/c_bottarisp.pdf
* Si suggerisce di svolgere anche gli esercizi 7.118, 7.119,7.121, 7.126, a pag. 90 delle dispense di G. Niesi http://www.dima.unige.it/~niesi/MD/a05/MD05appunti.pdf

RISPOSTE

NOMENCLATURA

Dato il numero complesso in forma algebrica z=a+ib, si definisce:

- parte reale di z: Re(z) = a
- parte immaginaria di z : Im(z) = b
- modulo di z : $|z| =\rho=\sqrt{a^2+b^2}$
- coniugato di z : $\overline{z}$ = a-ib

1.a) $Re(z)=\frac{9}{5}$, $Im(z)=-\frac{2}{5}$

1.b) $Re(z)=-\frac{1}{2}$, $Im(z)=\frac{\sqrt{3}}{2}$

2. a) $z=-\frac{i}{2}$, quindi $|z|=\frac{1}{2}$, $Arg(z)=-\frac{\pi}{2}$; b) z= 16+16i, quindi $|z|=16\sqrt{2}$, $Arg(z)=\frac{\pi}{4}$;
   c) usando De Moivre ... si trova $|z|=\frac{\sqrt{8}}{3}$, $Arg(z)=\frac{7\pi}{4}$

3. -3+0·i

4.a) $\sqrt{3}-1$, $2\sqrt{2}$, $\sqrt{2}$

4.b) $Arg(iz_1)=-\frac{4\pi}{6}$, $Arg\left(\frac{z_1}{z_2}\right)=-\frac{11\pi}{12}$, $Arg(3z_2)=-\frac{\pi}{4}$

5.a) $13(\cos\pi+i\,sen\pi)$

5.b) $\sqrt{2}\left(\cos\frac{\pi}{2}+i\,sen\frac{\pi}{2}\right)$

5.c) $8\left(\cos-\frac{\pi}{3}+i\,sen-\frac{\pi}{3}\right)$

6.c) I PASSO : Si scrivono numeratore e denominatore della base in forma trigonometrica :

$1+i\sqrt{3}=\ldots\ldots=2\left(\cos\frac{\pi}{3}+i\,sen\frac{\pi}{3}\right)$ e $1+i=\ldots\ldots=\sqrt{2}\left(\cos\frac{\pi}{4}+i\,sen\frac{\pi}{4}\right)$

II PASSO : Si effettua il quoto ottenendo $z=\sqrt{2}\left(\cos\frac{\pi}{12}+i\,sen\frac{\pi}{12}\right)$

III PASSO : Si calcola z^8 con la formula di De Moivre e si ottiene $z^8=\ldots=2^4\left(\cos\frac{2\pi}{3}+i\,sen\frac{2\pi}{3}\right)$

IV PASSO : Si sostituiscono i valori numerici del seno e coseno: si arriva al risultato $-8+8i\sqrt{3}$.

7. La somma vale zero. Raggruppare a 'gruppi di 4', tenendo conto che $i^5+i^6+i^7+i^8=0$