Agenda

- *Divisione in colonna*
- *Utili identità dimostrate tramite induzione*
- *Gruppi ed Anelli*
- *Z_2 Definizione assiomatica e operazioni logiche*
- *Z_n*

Esercizio “Divisione in colonna”

Divisione in colonna (Long division), in base decimale e binaria,

1325/17 1325=17*77+16

In bit 17 -> 1001= 16+1 1325 -> 10100101101

1325 ->1324/2=662 -> 331 -> 330/2=165 -> 164/2=82-> 41 ->

1 0 1 1 0 1

40/2=20 -> 20/2=10 -> 10/2=5 -> 4/2=2 -> 2/2=1

0 0 1 0 1

Esercizio “Divisione in colonna”

```
10100101101   |  10001
10001         |  1001101   -> 77
   11101      |
   10001      |
    11001     |
    10001     |
     100001   |
      10001   |
      10000 -> 16
```

Esercizio “Divisione in colonna”

1325	| 17	77 -> 1001101
119	| 77	
135	|	
119	|	
16		

77 -> 76/2=38 -> 38/2=19 -> 18/2=9 -> 8/2=4 -> 4/2=2 -> 2/2=1

1 0 1 1 0 0 1

Note sulla divisione in colonna

- *L'algoritmo può essere eseguito da una MdT*

- *La differenza è quasi uguale alla somma, ma il "riporto" segue una tabellina diversa:*

  1,1 -> 0; 1,0 -> 1; 0,1 -> 1; 0,0 -> 0

  (vedremo come ottenerlo)

Esercizio: fare similmente il prodotto in colonna.

Correzione Esercizio per casa

- *Dimostrare per induzione l'associatività del prodotto.*

$a \times (b \times c) = (a \times b) \times c$

Per induzione su c:

$a \times (b \times 0) = 0 = (a \times b) \times 0$ **(Caso c=0)**

$a \times (b \times s(c)) = a \times (b \times c + b) = a \times (b \times c) + a \times b =$

$= (a \times b) \times c + (a \times b) = (a \times b) \times c + (a \times b) \times 1 =$

$= (a \times b) \times (c + 1) = (a \times b) \times s(c)$ **(Ricorsione)**

Correzione Esercizio basi

- *Nella cartella BaseChange*

Trovate una codice Octave

Binaryrep.m

Che calcola e allinea le rappresentazioni in base 2, 4, 8, 16, 32

- *Trovate la funzione nextpow.m*

Che calcola il logaritmo intero di un numero naturale in una base.

Dimostrare la formula di Gauss

- *1 + 2 + … + n = n(n+1)/2=S*

Karl Friederic Gauss
1777 - 1855

- *Alle elementari …*

1 + 2 + 3 + … + N +

N +(N-1)+ (N-2)+ … + 1 =

(N+1)+(N+1)+… +(N+1) = 2S

-> S=(N+1)N/2 (N termini tutti (N-1)) OK

Soluzione formula di Gauss

- $1 + 2 + \ldots + n = n(n+1)/2$

Per induzione su n

- $1 = (1+1)(1)/2=1$ **(verifica caso n=1)**

- $1 + 2 + \ldots + n + n+1=n(n+1)/2 +n+1=(n+1+1)/2(n+1)=$

$= (n+2)(n+1)/2=((n+1)+1)(n+1)/2$ **(Ricorsione)**

Tartaglia

- ***Numeri di Tartaglia definiti per induzione***

$B(N,0)=B(N,N)=1$

$B(N,K)=B(N-1,k-1)+B(N-1,k)$

K	0	1	2	3	4	5	6	K è indice di colonna
0	1							N=0
1	1	1						N=1
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		N=5 N è indice di riga.
6	1	6	15	20	15	6	1	N=6 N è indice di riga.

Niccolò Tartaglia 1499-1557
Repubblica di Venezia

Triangolo di Tartaglia - Binomio di Newton

Tartaglia vs Bernoulli-Newton

- *Dimostrare per ispezione che la formula chiusa*

$$B(N,k)=\left(\begin{array}{c} N \\ k \end{array}\right)=\frac{N!}{(N-k)!k!}=\frac{N\cdot(N-1)\cdots(N-k+1)}{k\cdot(k-1)\cdots 2\cdot 1}$$

rispetta la regola di ricorrenza di Tartaglia

B(N,K)=B(N-1,k-1)+B(N-1,k)

$$\left(\begin{array}{c} N \\ k+1 \end{array}\right)=\left(\begin{array}{c} N-1 \\ k \end{array}\right)+\left(\begin{array}{c} N-1 \\ k+1 \end{array}\right)$$

$$\left(\begin{array}{c} N-1 \\ k \end{array}\right)+\left(\begin{array}{c} N-1 \\ k+1 \end{array}\right)=\frac{(N-1)\cdots(N-k)}{k\cdot(k-1)\cdots 2\cdot 1}+\frac{(N-1)\cdots(N-k-1+1)}{(k+1)\cdot k\cdot(k-1)\cdots 2\cdot 1}=$$

$$=\frac{(N-1)\cdots(N-k)}{(k+1)\cdot k\cdot(k-1)\cdots 2\cdot 1}[k+1+(N-k+1)]=\frac{(N-1)\cdots(N-k+1)}{(k+1)\cdot k\cdot(k-1)\cdots 2\cdot 1}=\left(\begin{array}{c} N \\ k+1 \end{array}\right)$$

Tartaglia

Dimostrare per induzione su N la formula

$$\sum_{k=0,N}\begin{pmatrix} k+2 \\ 2 \end{pmatrix}=\begin{pmatrix} N+3 \\ 3 \end{pmatrix}=(N+3)(N+2)(N+1)/6$$

K è indice di colonna

0	*1*	*N=0*
1	*1 1*	*N=1*
2	*1 2 1*	
3	*1 3 3 1*	
4	*1 4 6 4 1*	
5	*1 5 10 5 4 1*	*N=5 N è indice di riga.*

Numeri triangolari - Binomio di Newton

Niccolò Tartaglia

1499-1557

Repubblica di Venezia

- *Dimostrare per induzione su N la formula*

$$\sum_{k=0,N}\begin{pmatrix} k+P \\ P \end{pmatrix}=\begin{pmatrix} N+P+1 \\ P+1 \end{pmatrix}=(N+P)(N+p-1)\cdots(N+1)/P!$$

- ***(verifica caso N=0)***

$$\sum_{k=0,0}\begin{pmatrix} k+P \\ P \end{pmatrix}=\begin{pmatrix} 0+P \\ P \end{pmatrix}=1=\begin{pmatrix} 0+P+1 \\ P+1 \end{pmatrix}$$

- ***(Ricorsione=Legge di ricorrenza)***

$$\sum_{k=0,N+1}\begin{pmatrix} k+P \\ P \end{pmatrix}=\begin{pmatrix} N+P+1 \\ P+1 \end{pmatrix}+\begin{pmatrix} N+P+1 \\ P \end{pmatrix}=\begin{pmatrix} N+P+1+1 \\ P+1 \end{pmatrix}=\begin{pmatrix} (N+1)+P+1 \\ P+1 \end{pmatrix}$$

Somma dei cubi

- *Dimostrare che*

$$\sum_{k=0,N} k^3 = \left[(N+1)N/2\right]^2$$

Somma dei quadrati

- *Dimostrare che*

$$\sum_{k=0,N} k^2 = \sum_{k=0,N} k^2 - k + k = \sum_{k=0,N} k(k-1) + k = \sum_{k=0,N} 2\frac{1}{2}k(k-1) + k =$$

$$= \sum_{k=0,N} 2\frac{1}{2}k(k-1) + k = \sum_{k=0,N} 2\binom{k}{2} + k = 2\binom{N+1}{3} - \binom{N+1}{2}$$

$$2\binom{N+1}{3} - \binom{N+1}{2} = \frac{1}{3}(N+1)(N)(N-1) - \frac{1}{2}(N+1)(N) =$$

$$\frac{1}{6}(N+1)(N)[2(N-1)+3] = \frac{1}{6}(N+1)(N)[2N+1]$$

Esercizio Somma dei quadrati

- *Dimostrare che*

$$\sum_{k=0,N} k^2 = \frac{1}{6}(N+1)(N)[2N+1]$$

1+2^2=1+4=5=3x2x(2x2+1)x1/6

1+2^2+3^2=1+4+9=14=4x3x(2x3+1)x1/6=2x7=14

Serie Geometrica Induzione

- *Dimostriamo per induzione su N*

$$\sum_{k=0,N} a^k = \frac{1-a^{N+1}}{1-a}$$

- ***(verifica caso N=0)***

$$\sum_{k=0,0} a^k = a^0 = 1 = \frac{1-a^1}{1-a}$$

- ***(Ricorsione su N)***

$$\sum_{k=0,N+1} a^k = \sum_{k=0,N} a^k + a^{N+1} = \frac{1-a^{N+1}}{1-a} + a^{N+1} = \frac{1-a^{N+1}+a^{N+1}-a^{N+2}}{1-a} = \frac{1-a^{N+2}}{1-a}$$

Somma dei cubi

- *Dimostrare che* $\sum_{k=0,N} k^3 = \left[(N+1)N/2\right]^2$

$$\sum_{k=0,2} k^3 = 1+8 = 9 = \left[(2+1)2/2\right]^2 = \left[3\right]^2 = 9$$

(verifica caso N=2, 0 è banale 0=0)

$$\sum_{k=0,N+1} k^3 = \left[(N+1)N/2\right]^2 + (N+1)^3 =$$

$$= \left[(N+1)\right]^2 \left[\left(N/2\right)^2 + (N+1)\right] =$$

$$= \left[(N+1)/2\right]^2 \left[N^2 + 4(N+1)\right] =$$

$$= \left[(N+1)/2\right]^2 \left[(N+2)^2\right] = \left[(N+1)(N+1+1)/2\right]^2$$

- ***(Ricorsione)***

Gruppi

Un gruppo G è un insieme dotato di una operazione associativa w con elemento neutro unico e ed un inverso:

$$\forall a,b \in G : \exists w(a,b) \in G$$

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

$$\forall a \in G \Rightarrow \omega(a,e) = a = \omega(e,a)$$

$$\forall a \in G \Rightarrow \exists b = inv_{Sx}(a) : w(b,a) = e$$

Analogamente a Dx.

*Il gruppo si dice **abeliano** quando la sua operazione è commutativa.*

Semigruppi

Un semigruppo G è un insieme dotato di una operazione associativa w con elemento neutro unico:

$$\forall a,b \in G : \exists w(a,b) \in G$$

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

$$\forall a \in G \Rightarrow \omega(a,e) = a = \omega(e,a)$$

Non tutti gli elementi ammettono un inverso.

*Il semigruppo si dice **abeliano** quando la sua operazione è commutativa.*

I Naturali sono un semigruppo

- *Abbiamo visto che i naturali formano un semigruppo rispetto alla somma e rispetto al prodotto.*

- *Esistono gli elementi neutri per entrambe le operazioni. 0+a=a 1xa=a.*

- *I Naturali non formano un gruppo rispetto a nessuna delle due operazioni perché non esistono gli inversi.*

Anelli

Un anello è un gruppo abeliano rispetto ad una operazione detta ***somma*** *e dotato di una seconda operazione associativa detta* ***prodotto***

$$\forall a,b \in G : \exists ab \in G$$

$$a(bc) = (ab)c$$

che rispetta la ***proprietà distributiva****:*

$$(a+b)c = ac + bc$$

$$a(b+c) = ab + ac$$

*Quando il prodotto è commutativo l'****anello*** *si dice* ***abeliano***

Anelli con unità

Un anello K si dice "con unità" I quando il prodotto ammette un elemento neutro unico.

$$\forall a \in K : \exists a + b \in K \vee \exists ab \in K$$

$$\exists I \forall a \in K : aI = Ia = a$$

Anelli abeliani Ciclici

*Sono insiemi di numeri che sodisfano tutte le proprietà (di Peano) precedenti, ma **esiste un elemento che precede lo zero** e quindi non vale la relazione d'ordine*

$$\exists a > 0 : a + 1 = 0 \Rightarrow a + 1 = 0 < a$$

Viceversa i naturali, si ottengono imponendo che non esista il precedente dello zero. Ogni numero è diverso dai precedenti:

n+1=m (n-m)+m+1=m (n-m+1)+m=m n-m+1=0

Se rimuoviamo l'ipotesi che a+1 sia diverso da a la situazione diviene più complessa

Esempi:

1+1=0 Si chiama Z_2 e possiede solo due elementi (0,1)

Vedremo che è un campo

Anelli abeliani Ciclici

Esempio:

Esite 1+1 diverso da 0 che chiamiamo 2.

2+1=0

Vedremo che è un campo (un gruppo per la somma e per il prodotto escludendo lo zero)

L'opp di 1 è 2 e viceversa. L'inverso di 2 è 2:

2x2=2(1+1)=2+2=2+(1+1)=0+1=1

Si chiama Z_3

In generale se si interrompe la catena al passo n si ottiene Z_n *che è sempre un anello commutativo con unità, ma non sempre un campo. (esercizi)*

Tabelline

- *Per Z_2 è definito da [s(1)=1+1=0]*

Somma: 0+a=a; 1+1=0

a+b	0	1
0	0	1
1	1	0

Prodotto

0 x a= 0

1 x a=1

axb	0	1
0	0	0
1	0	1

Quali sono tutte le operazioni in Z_2?

- *Sono 2^4=16 (possibili risposte)*
- *Operazioni E (AND), O-Vel (OR), O-Aut (XOR)*

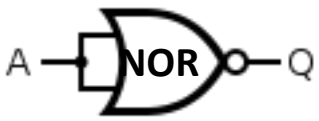
A	B	A.AND.B
0	0	0
0	1	0
1	0	0
1	1	1

A	B	A.OR.B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	A.XOR.B
0	0	0
0	1	1
1	0	1
1	1	0

A	B	A.NOR.B
0	0	1
0	1	0
1	0	0
1	1	0

- *Somma? Si coincide con XOR*
- *Prodotto? Si coincide con AND*



Quali sono tutte le operazioni in Z_2?

- *Tabellina Somma in Z_2*

A	B	A.XOR.B
0	0	0
0	1	1
1	0	1
1	1	0

a	b	a+b
0	0	0
0	1	1
1	0	1
1	1	0

a+b	0	1
0	0	1
1	1	0

- *Tabellina Prodotto in Z_2*

A	B	A.AND.B
0	0	0
0	1	0
1	0	0
1	1	1

a	a	a x b
0	0	0
0	1	0
1	0	0
1	1	1

axb	0	1
0	0	0
1	0	1

Spazi di due elementi: tutte le operazioni

A	B	False
0	0	0
0	1	0
1	0	0
1	1	0

A	B	A.AND.B
0	0	0
0	1	0
1	0	0
1	1	1

A	B	A.XOR.B
0	0	0
0	1	1
1	0	1
1	1	0

A	B	A.OR.B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	A.AND.\B
0	0	0
0	1	0
1	0	1
1	1	0

A	B	A
0	0	0
0	1	0
1	0	1
1	1	1

A	B	\A.AND.B
0	0	0
0	1	1
1	0	0
1	1	0

A	B	B
0	0	0
0	1	1
1	0	0
1	1	1

Spazi di due elementi: tutte le operazioni

A	B	A.NOR.B
0	0	1
0	1	0
1	0	0
1	1	0

A	B	A==B
0	0	1
0	1	0
1	0	0
1	1	1

A	B	A.NAND.B
0	0	1
0	1	1
1	0	1
1	1	0

A	B	True
0	0	1
0	1	1
1	0	1
1	1	1

A	B	\B
0	0	1
0	1	0
1	0	1
1	1	0

A	B	A<-B
0	0	1
0	1	0
1	0	1
1	1	1

A	B	\A
0	0	1
0	1	1
1	0	0
1	1	0

A	B	A->B
0	0	1
0	1	1
1	0	0
1	1	1

Anelli abeliani Ciclici Z_n

Assiomi:

(N, s, 0): N è un insieme di numeri.

*- Esiste **0** in N*

- *Per ogni numero esiste il **successivo**.*
- ~~***0** non è successivo di nessun numero (non ha precedenti).*~~
- ***Esiste b il cui successore è lo 0**. s(b)=0.*
- *(**Iniettività successivo**). Se i successivi di sue numeri sono uguali allora i numeri sono uguali. [Unicità del predecessore)]*
- *(**Induzione**) Tutti i numeri sono ottenibili reiterando l'operazione di successivo a partire dall'unità. Ovvero Se un insieme contiene 0 ed è chiuso rispetto al successivo coincide con tutto N.*
- *(**Induzione**) Se una proprietà è verificata per lo zero e fissata vera per un numero è vera per il successivo, allora è vera in tutto N.*

A(0) vera e [A(n) vera -> A(s(n)) vera] implica A(k) vera su tutto N.

Anelli abeliani Ciclici

Dobbiamo dimostrare che è un anello. Le due operazioni di somma e prodotto si definiscono analogamente alla costruzione per i naturali, ma dobbiamo dimostrare che l'insieme è dotato di ***opposto*** *(inverso rispetto alla somma) e quindi forma un* ***gruppo rispetto alla somma****.*

- *1=s(0) (per definizione) quindi s(a)=a+1.*
- ***1*** *ha un* ***opposto*** *il precedente dello zero: s(b)=b+1=0.* ***b=-1***
- *Se esiste l'opposto di a: a+(-a)=0, allora esiste l'opposto del successivo di a: a+1+b+(-a)=0; s(a)+(b+(-a))=0*
- *(-a+b) è opposto del successivo di a=s(a).*

- *Quindi se a ha un opposto lo ha anche il suo successivo. Per induzione segue che* ***tutti gli elementi di Z_n hanno un opposto****.*

Messaggio

Usando solo una serie appropriata di xor una macchina di Touring può eseguire la divisione (in colonna).[Base per la crittografia moderna]

Abbiamo introdotto i concetti di ***Gruppo*** *ed* ***Anello***

Abbiamo costruito assiomaticamente gli anelli ciclici abeliani Z_n

Abbiamo analizzato in dettaglio tutte le possibili operazioni in Z_2 *e la loro corrispondenza nel formalismo della* ***logica****.*