La “Signora degli Anelli”

*Ad “**Emmy Noether**” si devono molti risultati in teoria dei numeri ed in particolare sugli ideali gli anelli “Ring” a cui ha dato il nome.*

Amalie Emmy Noether *nata il 23 Marzo 1882*

- *Erlangen, Bavaria, Impero Germanico*

Morta il14 Aprile 1935 (aged 53) a Bryn Mawr, Pennsylvania, USA.

(tratto da wikipedia – da usare solo per le informazioni, non per la teoria)

Anello (in sintesi)

Un anello è uno spazio dotato di una operazione abeliana detta ***somma*** *rispetto a cui forma un* ***gruppo*** *ed una seconda operazione detta* ***prodotto***, ***associativa*** *e* ***distributiva*** *rispetto alla somma.*

Gli attributi degli anelli corrispondono a proprietà del prodotto:

*Quando esiste l'elemento neutro rispetto al prodotto l'anello è detto "****con unità****".*

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

Corpi e Campi

Un corpo è un anello che privato dell'elemento neutro rispetto alla somma costituisce un gruppo rispetto al prodotto

$$\exists 1 : a1 = 1a = a$$

$$\forall a \neq 0 \in G : \exists (a)^{-1} \in G : a(a)^{-1} = (a)^{-1} a = 1$$

L'elemento neutro rispetto al prodotto è detto unità.

Un campo è un corpo commutativo cioè dotato di un prodotto commutativo.

Vediamo Z_n

Definizione:

Z_n possiede n elementi distinti. "Zahl-ringe"

$$Z_n = \{0,1,2,\cdots,n-1\}$$

Esiste uno ed un solo numero il cui successivo è 0.

Somma:

0 + a=a

Se a+b < n la somma si eredita dai naturali N.

Se in N a+b>=n a+b in Zn =a+b-n.

Vediamo Z_n

Se in N $a+b>=n$ $a+b$ *in* $Z_n = a+b-n$. $Z_n = S$

In sintesi $(a+b)_S = mod(a+b,n)$

La funzione mod(a,b) corrisponde alla funzione "rem" in Octave ed indica il resto della divisione di a rispetto a b.

Se $a=bq+r$ $mod(a,b)=r$

Analogamente la divisione sugli interi è il quoziente

"a/b"=q

Vediamo Z_n

Definizione:

Z_n possiede n elementi distinti in corrispondenza biunivoca con i numeri naturali 0,1,…,n-1.

Il successivo di n-1 è 0.

Somma:

$0 + a = a$

Se $a_{in\ N} + b_{in\ N} < n$ la somma si eredita da N: $a_{in\ N} + b_{in\ N} = a+b$.

Se $(a)_{in\ N} + (b)_{in\ N} = n$; $a+b = a+b-1+1 = n-1+1 = 0$ (Esiste opposto)

Se $(a)_{in\ N} + (b)_{in\ N} > n$; $a+b = (a+b)-(n-1)-1 = (a+b)_{in\ N} - n$

In generale $a+b = mod((a+b)_{in\ N}, n)$

Vediamo Z_n

Prodotto:

$$a \times b = mod((a_{in\ N} \times b_{in\ N}), n)$$

Induzione su b

$$a \times 0 = 0 = mod((a_{in\ N} \times 0), n) = 0$$

$$a \times (b+1) = a \times b + a = mod((a_{in\ N} \times b_{in\ N}), n) + a =$$

$$= mod((a_{in\ N} \times b_{in\ N}) + a_{in\ N}, n) =$$

$$mod((a_{in\ N} \times (b+1)_{in\ N}), n)$$

Quindi Z_n è un ***anello con unità.***

Nozione di Equivalenza

Una relazione di equivalenza deve godere delle proprietà:

$a \sim a$	*(Riflessiva)*
$a \sim b \rightarrow b \sim a$	*(Simmetrica)*
$a \sim b$ e $b \sim c \rightarrow a \sim c$	*(Transitiva)*

Es: l'uguaglianza =, "la somma è pari",

"Essere germani cioè avere due genitori in comune"...

Nozione di Equivalenza

Uguaglianza

$a = a$ *(Riflessiva)*

$a = b \rightarrow b = a$ *(Simmetrica)*

$a = b \; e \; b = c \rightarrow a = c$ *(Transitiva)*

Nozione di Equivalenza

"La somma pari"

$a + a = 2\,a \quad$ *pari* *(Riflessiva)*

$a + b = 2\,n \rightarrow b + a = 2n$ *(Simmetrica)*

$a + b = 2n$ *e* $b + c = 2m \rightarrow$

$a + b + b + c = 2n + 2m$

$a + 2b + c = 2(n+m)$

$a + c = 2(n+m-b)$ *(Transitiva)*

La somma è dispari

Non è una equivalenza

$a + a = 2a$ *è pari non dispari* *(Riflessiva)*

Relazione d'ordine

Non è una equivalenza

$a > a$ è falsa. *(Riflessiva)*

Relazione d'ordine parziale

Questa non è una equivalenza

$a >= a$ *è vera* $(a=a)$ *(Riflessiva)*

$a >= b \rightarrow b >= a$ (*falsa tranne per* $a=b$) *(Simmetrica)*

$a >= b$ *e* $b = c$ -> $a >= c$ *(Transitiva)*

Ineguaglianza Diversità

Non è una equivalenza

a non è diversa da a

Cuginanza

"Cugini sono individui con due nonni in comune".

Non è una equivalenza:

Ognuno è cugino di se stesso ***(Riflessiva)***

Se a è cugino di b, b è necessariamente cugino di a.

(Simmetrica)

Se a è cugino di b, e b è cugino di c; c può avere gli altri 4 nonni. Esempio: ***(Transitiva)***

Nonni di a: $n_1\ n_2\ n_3\ n_4$
Nonni di b: $n_3\ n_4\ n_5\ n_6$
Nonni di c: $n_1\ n_2\ n_5\ n_6$

Classi

- *Gli elementi equivalenti in un insieme formano una partizione in **classi**.*

- *Un elemento che appartiene ad una classe si dice un suo **rappresentante**.*

Classi dei resti

- *Due elementi sono equivalenti in N se la loro differenza è un multiplo di un numero fisso n.*

- *Definizione equivalente:*

Due elementi sono equivalenti se il loro resto rispetto alla divisione per n è lo stesso.

- Le definizioni coincidono.

$a = q \times n + r \quad b = p \times n + r \rightarrow a - b = (q - p) \times n$

Somma tra classi

- *La somma tra due classi è la classe (unica) a cui appartiene la somma dei rappresentanti.*

Bisogna dimostrare che non dipende dal rappresentante:

$Cl\,(a) + Cl\,(b) = Cl\,(a+b)$

$a=q\,n + r \quad b= p\,n + s \quad a+b= (q+p)\,n + r+s= (q+p+[r+s])\,n + mod\,(r+s)$

Le classi sono in corrispondenza biunivoca con i loro rappresentanti minori di n.

Prodotto tra classi

- *Il prodotto tra due classi è la classe (unica) a cui appartiene il prodotto dei rappresentanti.*

Bisogna dimostrare che non dipende dal rappresentante:

$$Cl(a) \times Cl(b) = Cl(axb)$$

$$a = q\,n + r \quad b = p\,n + s \quad ab = (qp)\,n^2 + (rp+sq)n + rs =$$

$$= (qp)\,n^2 + (rp+sq)n + [rs/n]n + mod(r\,s)$$

Prodotto tra classi

La collezione delle classi forma lo "Spazio Quoziente"

Le classi sono in corrispondenza biunivoca con (0,1,2…n-1) elementi di Z_n.

Inoltre la somma ed il prodotto coincidono con quelli definiti in Z_n.

Dunque le classi dei resti modulo n e Z_n *sono* ***isomorfe***.

Tassonomia delle applicazioni

*Un'**applicazione** è una legge (una regola) che associa ad elementi di uno spazio, detto "**Dominio**", elementi di un altro spazio detto "**codominio**".*

T: D -> C

*L'elemento associato nel codominio si dice "**immagine**".*

*L'elemento associato (o l'insieme degli elementi associati) nel dominio si dice "**controimmaggine**".*

*Un'applicazione tra due spazi si dice "**iniettiva**" quando trasforma elementi distinti in elementi distinti.*

*Un'applicazione tra due spazi si dice "**suriettiva**" quando tutti gli elementi del codominio posseggono una contro-immagine.*

*Una applicazione si dice bigettiva o **biettiva** (bi-iettiva) quando iniettiva e suriettiva.*

Tassonomia delle applicazioni

*Un **morfismo** (dal greco morf , morph, che significa forma) è una applicazione tra due spazi che ne preserva la struttura cioè le (alcune delle) proprietà di cui godono.*

*Un **omomorfismo** (dal greco omoc omos, che significa stesso) è una applicazione univoca tra due spazi che ne preserva la struttura cioè tutte le proprietà di cui godono. [Monodroma].*

*Un **isomorfismo** (dal greco isoc isos, che significa uguale) e una applicazione biunivoca tra due spazi che ne preserva la struttura cioè tutte le propriet`a di cui godono. In pratica un omomorfismo invertibile.*

*Un **endomorfismo** è un morfismo di uno spazio in se stesso.*

*Un **automorfismo** è un isomorfismo interno*

*Un **monomorfismo** è un morfismo iniettivo*

*Un **epimorfismo** è un morfismo suriettivo*

Esercizio

- *Scrivere la tabellina del prodotto dei primi Zn con n=3,5,6,7,10,11,12,13…*

I Naturali sono un semigruppo

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

- *Nella somma esiste elemento neutro*

$a+0=a$

Gli Interi

Possiamo allargare il semi-anello dei naturali per renderlo un gruppo rispetto alla somma?

- *Mancano solo gli inversi rispetto alla somma cioè gli "**opposti**":*

a + inv(a) = 0. (tranne per lo zero 0 + 0=0)

- *Definiamo **j='-1' opposto di 1**: 1 + j=1+(-1) = 0 (coerente con la differenza)*

- *-1 + (-1) =? Può dare un naturale? No (il suo successivo sarebbe -1). Quindi è un nuovo numero. Inoltre -1 + (-1) + 2 = -1 + (-1) + 1 + 1= -1 + 0 + 1= -1 + 1 = 0 è l'opposto di 2. lo chiamiamo quindi -2 etc.*

Gli Interi – Predecessore dello zero

*Gli interi si indicano con il simbolo **Z** (dal tedesco Zahl).*

In generale se cambiamo l'ipotesi di Peano:

"Lo zero non ammette predecessori" in "Lo zero non ammette predecessori in N"

*"Esiste il predecessore **j** dello zero s(j)=0"*

Lemma "j è l'opposto di 1"

$s(j)=s(j+0)=j+s(0)=j+1.$

Gli Interi - Opposti

Th "Tutti i naturali hanno l'opposto"

Per induzione su a

0+0=0; opp(o)=-0=0; **(a=0)**

Se –a esiste esiste l'opposto di a+1 **(Ricorsione)**

a+ (-a) = 0; a+1 +(-1)+(-a)= s(a)+[-1+(-a)]=0

Gli Interi negativi

Per definizione gli interi negativi ***Z_*** *sono definiti dalle due proposizioni:*

-1 *è un elemento (esistenza opposto di 1)*

Se un elemento a fa parte degli ***interi negativi*** *ne fa parte anche il "****precedente****" cioè a + (-1).*

(chiusura rispetto alla somma).

Siccome gli assiomi sono identici a quelli di N, l'insieme ***Z_*** *è isomorfo ad N. I numeri di Z_ in Z si dicono "****negativi****".*

Gli Interi negativi: precedente

*Il **precedente** dell'opposto è l'opposto del successivo:*

Per induzione su a

-1 = 0 + (-1) è precedente di 0.

-1 + 1 = 0 **(Caso a=0)**

Prec(a)= -1 + a; *prec(a) + s(inv(a))=*

prec(a) + 1 + inv(a) = a + (-1) + 1 – inv(a) = 0

(Ricorsione)

Somma su Z

Si definisce tramite tre casi:

1) a, b naturali a+b è il naturale a + b.

2) a naturale b negativo: b = -c due casi:

i) a > c a+b = a-c

ii) a < c a +b = -(c-a)

3) a e b negativi a = -c, b = -d -> a+b =- (c+d)

*Z forma un **gruppo rispetto alla somma**.*

*Z^+ e Z^- sono isomorfi as N. **Z è un Anello***

Prodotto su Z

Si definisce imponendo che il prodotto rispetti quello sui naturali e le proprietà associativa e distributiva.

Per gli altri casi (numero negativo per positivo o negativi tra loro) si ricava "regola dei segni" (-1)x(1)=-1; (-1)x(-1)=1

(-1)x(1)=-1 si ricava dalla distributiva

ax(0)=0 ax(1+-1)=a+ax(-1)=0 quindi ax(-1)=-a

(-1)x(-1)=1 si ricava dalla distributiva

(-1)x(-1+1)=0 -1x(+1-1)=-1+(-1)x(-1)=0 -> (-1)x(-1)=1

Messaggio

Gli anelli Z_n *sono una struttura naturale ottenibile sia assiomaticamente (modificando assiomi di Peano) che come* ***classi dei resti*** *delle congruenze.*

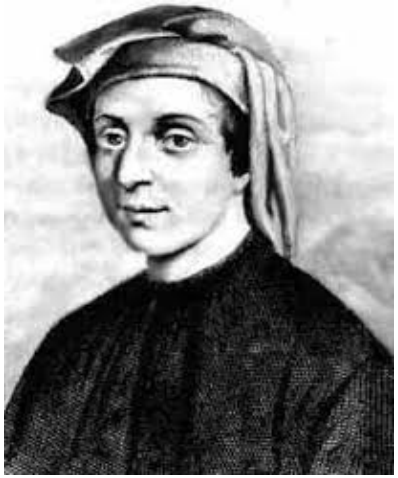
Z, l'insieme dei numeri ***Interi Relativi*** *si ottiene completando l'insieme dei naturali ovvero introducendo gli opposti (basta introdurre l'opposto dell'unità). Z è un'anello commutativo con unità.*

Abbiamo visto dagli esercizi le tabelline dei prodotti di alcuni Z_n. *Il prodotto di due numeri in* Z_n *può annullarsi senza che nessuno dei due sia nullo.*

Es: $0=3x2$ *(in* Z_6*);* $0=4x5$ *(in* Z_{10}*) etc*

Numeri di Fibonacci

I numeri di fibonacci si definiscono Induttivamente:



Pisa 1175-1235

- $N_1=0;\ N_2=1$ *(Definizioni k=1,2)*
- $N_{k+2}=N_k+N_{k+1}$ *(Ricorrenza su k)*

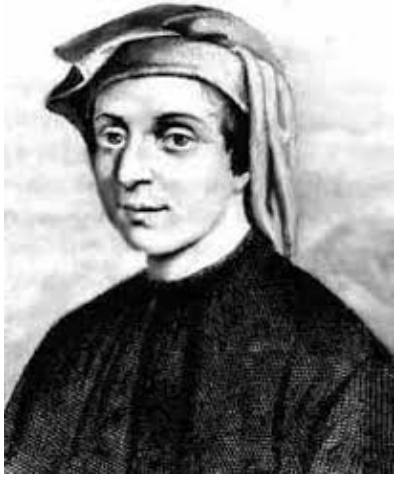
Numeri di Fibonacci

I numeri di fibonacci si definiscono

Induttivamente:

A) Scrivere codice Octave

B) Verificare per induzione forma chiusa



Pisa 1175-1235

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n}-\left(\frac{1-\sqrt{5}}{2}\right)^{n}\right]$$

- $N_1=0;\ N_2=1$ *(Definizioni k=1,2)*
- $N_{k+2}=N_k+N_{k+1}$ *(Ricorsione su K)*

Esercizi

- *Disegnare una MdT ad un nastro che esegue il confronto tra due naturali*
- *Disegnare un circuito che restituisce*

  1 se a>b, 0 a <b, 2 a=b

- *Disegnare una MdT che calcola la differenza*
- *Disegnare una circuito che restituisce (numeri a 4 bit): 1) a+b, 2) a-b 3) a/2, 4) mod(a,2), a/b, mod(a,b)*

Correzione Esercizio per casa

Dimostrare per induzione l'associatività del prodotto.

$a \times (b \times c) = (a \times b) \times c$ *induzione su c:*

$a \times (b \times 0) = a \times 0 = 0 = (a \times b) \times 0$ **(c=0 è vera)**

$a \times (b \times \mathbf{s(c)}) = a \times (b \times c + b) =$ **(c -> s(c))**

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

$= (a \times b) \times (c + 1) = (a \times b) \times \mathbf{s(c)}.$

Esercizio cambiamento di base

In gordion… BaseChange trovare vari esempi.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	10	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	11	10	3	3	3	3	3	3	3	3	3	3	3	3	3
4	100	11	10	4	4	4	4	4	4	4	4	4	4	4	4
5	101	12	11	10	5	5	5	5	5	5	5	5	5	5	5
6	110	20	12	11	10	6	6	6	6	6	6	6	6	6	6
7	111	21	13	12	11	10	7	7	7	7	7	7	7	7	7
8	1000	22	20	13	12	11	10	8	8	8	8	8	8	8	8
9	1001	100	21	14	13	12	11	10	9	9	9	9	9	9	9
10	1010	101	22	20	14	13	12	11	10	A	A	A	A	A	A
11	1011	102	23	21	15	14	13	12	11	10	B	B	B	B	B
12	1100	110	30	22	20	15	14	13	12	11	10	C	C	C	C
13	1101	111	31	23	21	16	15	14	13	12	11	10	D	D	D
14	1110	112	32	24	22	20	16	15	14	13	12	11	10	E	E
15	1111	120	33	30	23	21	17	16	15	14	13	12	11	10	F
16	10000	121	100	31	24	22	20	17	16	15	14	13	12	11	10
17	10001	122	101	32	25	23	21	18	17	16	15	14	13	12	11
18	10010	200	102	33	30	24	22	20	18	17	16	15	14	13	12
19	10011	201	103	34	31	25	23	21	19	18	17	16	15	14	13
20	10100	202	110	40	32	26	24	22	20	19	18	17	16	15	14
21	10101	210	111	41	33	30	25	23	21	1A	19	18	17	16	15
22	10110	211	112	42	34	31	26	24	22	20	1A	19	18	17	16
23	10111	212	113	43	35	32	27	25	23	21	1B	1A	19	18	17
24	11000	220	120	44	40	33	30	26	24	22	20	1B	1A	19	18
25	11001	221	121	100	41	34	31	27	25	23	21	1C	1B	1A	19
26	11010	222	122	101	42	35	32	28	26	24	22	20	1C	1B	1A
27	11011	1000	123	102	43	36	33	30	27	25	23	21	1D	1C	1B
28	11100	1001	130	103	44	40	34	31	28	26	24	22	20	1D	1C
29	11101	1002	131	104	45	41	35	32	29	27	25	23	21	1E	1D
30	11110	1010	132	110	50	42	36	33	30	28	26	24	22	20	1E
31	11111	1011	133	111	51	43	37	34	31	29	27	25	23	21	1F

I numeri da 0 a 31 nelle basi da 2 a 16

La base decimale è riportat anche all'inizio.

Le lettere ABCDEF sono utilizzate per I simboli nelle basi maggiori di 10:

A=10, B=11, C=12…