

ALMA MATER STUDIORUM · UNIVERSITÀ DI
BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea Triennale in Matematica

Partizioni di un intero

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof
Libero Verardi

Presentata da:
Giorgia Lari

Seconda sessione
Anno Accademico 2012-2013

*A mia nonna,
Giselda.*

Introduzione

Questa tesi di laurea tratta delle partizioni di un intero positivo.

La tesi viene suddivisa in tre capitoli: nel primo capitolo definirò cosa significa scomporre additivamente un intero positivo e come si può rappresentare una partizione cioè utilizzando diagrammi, chiamati *diagrammi di Ferrers*, o tabelle, chiamate *tableau di Young*, si possono rappresentare graficamente partizioni. In seguito, in questo capitolo, verrà definita la funzione di partizione e, infine, tratterò delle partizioni ordinate. Il secondo capitolo ha carattere storico: infatti, mostra come cinque famosi matematici, Eulero, Ramanujan e Hardy, Hans Rademacher e Ken Ono, nel tempo abbiano affrontato il problema di trovare una formula matematica che meglio rappresenti la funzione di partizione. Il terzo ed ultimo capitolo riguarda le applicazioni delle partizioni, cioè come esse abbiano una relazione con le classi di coniugio nel gruppo simmetrico S_n e con le classificazioni dei gruppi abeliani di ordine p^n , con p un numero primo.

Di alcune affermazioni (o teoremi) nei capitoli seguenti non è stata riportata la dimostrazione; in questi casi si rimanda direttamente alle corrispondenti citazioni bibliografiche.

Indice

1	Definizioni e proprietà	5
1.1	Partizione di un numero intero positivo	5
1.2	Le rappresentazioni di una partizione	9
1.3	La funzione di partizione	11
1.4	Partizioni ordinate	15
2	Storia	21
2.1	Eulero e le infinite partizioni	22
2.2	Ramanujan e Hardy	23
2.3	Hans Rademacher	26
2.4	Ken Ono e i frattali	28
3	Applicazioni	33
3.1	Le classi di coniugio nel gruppo simmetrico S_n	33
3.1.1	I gruppi e il coniugio	33
3.1.2	I gruppi di permutazioni e il coniugio	36
3.2	La classificazione dei gruppi abeliani di ordine p^n , con p primo	41
	Bibliografia	45
	Ringraziamenti	47

Capitolo 1

Definizioni e proprietà

*”Cosa significa scrivere 5 come somma di numeri interi positivi?
E in quanti modi si può scrivere 5 come somma di numeri interi positivi?”*

In questo primo capitolo risponderò a queste domande, cioè tratterò della partizione di un numero intero e delle sue rappresentazioni, poi, definirò la funzione di partizione, ovvero la funzione per mezzo della quale si può calcolare il numero di modi possibili per scrivere un intero positivo e, infine, tratterò delle partizioni ordinate (si è fatto riferimento a [10] e [7]).

1.1 Partizione di un numero intero positivo

Definizione 1.1. Una **partizione** di un intero positivo n è un modo di scrivere n come somma di interi positivi, senza tener conto dell'ordine degli addendi.

Formalmente, una partizione di n è una sequenza di interi positivi $\lambda_1, \lambda_2, \dots, \lambda_k$ tali che

$$\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$$

e

$$\sum_{i=1}^k \lambda_i = \lambda_1 + \lambda_2 + \dots + \lambda_k = n.$$

dove le componenti della sequenza, λ_i , sono dette **addendi** della partizione dell'intero n e la lunghezza della sequenza, k , viene chiamata **numero degli addendi** di n per il quale deve essere $1 \leq k \leq n$.

Definizione 1.2. Indicando con \mathbb{B} l'insieme delle partizioni dei vari interi positivi, spesso si scrive

$$\lambda = [\lambda_1, \lambda_2, \dots, \lambda_k] \in \mathbb{B} \quad (1.1)$$

per indicare che la sequenza $\langle \lambda_1, \lambda_2, \dots, \lambda_k \rangle$ è una partizione dell'intero positivo

$$n := \sum_{i=1}^k \lambda_i \quad (1.2)$$

e la scrittura (1.2) viene chiamata **rappresentazione canonica** della partizione dell'intero positivo.

Questa rappresentazione evidenzia il fatto che ogni partizione di un intero positivo si può identificare in una funzione non decrescente (che identifica un multinsieme) definita nel seguente modo

$$\mathbb{P} \rightarrow \mathbb{P}$$

$$(r] \mapsto (s]$$

dove $(r] = \{1, 2, \dots, r\}$ e $(s] = \{1, 2, \dots, s\}$ con r e s interi positivi.

Esempio 1.1. 0 ha una sola partizione:

$$0$$

Esempio 1.2. Le partizioni di 3 sono, invece, le seguenti:

$$3$$

$$1 + 2$$

$$1 + 1 + 1$$

Esempio 1.3. Le partizioni di 4 sono le seguenti:

$$\begin{aligned}
 &4 \\
 &3 + 1 \\
 &2 + 2 \\
 &2 + 1 + 1 \\
 &1 + 1 + 1 + 1
 \end{aligned}$$

Definizione 1.3. Un altro modo per rappresentare una partizione di un intero positivo è dato dalla **rappresentazione esponenziale**:

$$\lambda = \lambda_{(1)}^{h_1} \dots \lambda_{(m)}^{h_m} \quad (1.3)$$

con $\lambda_{(1)} > \lambda_{(2)} > \dots > \lambda_{(m)} > 0$, $h_1, h_2, \dots, h_m \in \mathbb{P}$.

Per ogni $i = 1, \dots, m$ l'intero h_i dice che la partizione dell'intero positivo n presenta h_i addendi uguali a $\lambda_{(i)}$; esso viene detto **molteplicità** di $\lambda_{(i)}$.

Chiaramente deve essere:

$$\sum_{i=1}^m h_i \lambda_{(i)} = n \quad (1.4)$$

e

$$\sum_{i=1}^m h_i = k \quad (1.5)$$

Con (1.5) si ricava il numero degli addendi.

Esempio 1.4. La rappresentazione canonica della partizione di 17 in 6 addendi è

$$\lambda = [5, 4, 4, 2, 1, 1]$$

cioè

$$17 = 5 + 4 + 4 + 2 + 1 + 1$$

mentre la sua rappresentazione esponenziale è

$$\lambda = 5^1 4^2 2^1 1^2$$

e utilizzando (1.4) si trova

$$\sum_{i=1}^6 h_i \lambda_{(i)} = 5 \cdot 1 + 4 \cdot 2 + 2 \cdot 1 + 1 \cdot 2 = 17$$

Definizione 1.4. Una partizione di un intero positivo si dice **partizione semplice** (o **partizione iniettiva**) se e solo se tutti i suoi addendi sono distinti, cioè se e solo se la funzione $\mathbb{P} \rightarrow \mathbb{P}$ è iniettiva, ossia se e solo se tutte le sue molteplicità sono uguali a 1.

Per una tale partizione

$$\lambda = [\lambda_1, \lambda_2, \dots, \lambda_k] = \lambda_1^{h_1} \dots \lambda_m^{h_m} \quad (1.6)$$

si ha

$$m = k \quad (1.7)$$

e $\forall i = 1, \dots, k$ tali che

$$\lambda_i = \lambda_{(i)}, \lambda_i = 1. \quad (1.8)$$

Esempio 1.5. Le partizioni di 6 sono:

$$[6] [5, 1] [4, 1, 1] [3, 1, 1, 1]$$

$$[2, 1, 1, 1, 1] [1, 1, 1, 1, 1, 1] [4, 2] [3, 2, 1]$$

$$[2, 2, 1, 1] [3, 3] [2, 2, 2]$$

e le partizioni semplici sono:

$$[6] [5, 1] [4, 2] [3, 2, 1].$$

1.2 Le rappresentazioni di una partizione

Per poter visualizzare una singola partizione di un certo numero in modo immediato, si possono utilizzare due metodi: *diagramma di Ferrers* e *tableau di Young*.

Definizione 1.5. Un **diagramma di Ferrers** di una partizione $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_k]$ di un intero positivo n con:

$$n := \sum_{i=1}^k \lambda_i$$

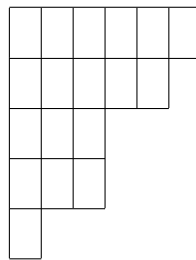
e viene denotato con $\mathfrak{F}(\lambda)$, il sottoinsieme della scacchiera completa $n \times n$ formato dalle prime λ_1 caselle della prima riga, dalle prime λ_2 caselle della seconda riga, \dots , dalle prime λ_k caselle della k -esima riga:

$$\mathfrak{F}(\lambda) := \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i \leq k, 1 \leq j \leq \lambda_i\}.$$

Esempio 1.6. Considero la partizione seguente

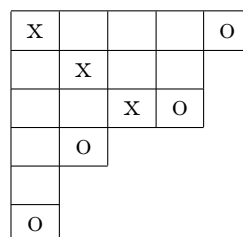
$$[6, 4, 3, 3, 1]$$

la sua rappresentazione di Ferrers è



Considero la seguente rappresentazione di Ferrers della partizione

$$\lambda = [5, 4, 4, 2, 1, 1]$$



Le caselle $(1, 1)$, $(2, 2)$, $(3, 3)$ (cioè quelle che sono riempite con una "x") compongono la *diagonale*, mentre $(1, 5)$, $(3, 4)$, $(4, 2)$ e $(6, 1)$ (cioè quelle che sono riempite con una "o") vengono chiamate *caselle d'angolo*.

In particolare, le caselle d'angolo di una forma di Ferrers di n sono tutte e sole le caselle la cui eliminazione porta ad una forma di Ferrers di $n - 1$. Mentre, aggiungendo alla forma di Ferrers caselle sotto le caselle $(1, 5)$, $(3, 4)$, $(3, 3)$, $(6, 1)$ e a destra della casella $(6, 1)$ si ottiene una forma di Ferrers di $n + 1$.

Definizione 1.6. Sia $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_k]$ una partizione di un intero n positivo e sia $\mathfrak{F}(\lambda)$ la sua forma di Ferrers, si definisce **tableau di Young** della partizione λ una funzione che ha dominio $\mathfrak{F}(\lambda)$.

Definizione 1.7. Sia $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_k]$ una partizione di un intero n positivo e sia $\mathfrak{F}(\lambda)$ la sua forma di Ferrers, si definisce **tableau di Young standard** della partizione λ una funzione biettiva così definita

$$\mathfrak{F} \leftrightarrow (n) \quad (1.9)$$

con $y \in \mathfrak{F}(\lambda)$ tali che gli $y_{i,j}$ presenti nelle righe e nelle colonne formino sequenze crescenti, cioè

$$\forall (i, j) \in \mathfrak{F}(\lambda) \text{ tali che } y_{i,j} < y_{i+1,j} \quad y_{i,j} < y_{i,j+1}. \quad (1.10)$$

Il seguente esempio è una applicazione della definizione appena data.

Esempio 1.7. Considero la partizione $\lambda = [3, 2]$ e costruisco le tavole di Young cioè devo collocare 1, 2, 3, 4 e 5 nelle caselle della forma di Ferrers in modo tale che in ogni riga e colonna si abbiano successioni crescenti.

Nelle caselle d'angolo colloco il numero più grande che in questo caso è 5 e così ottengo:

		5

	5	

Ora mi manca da collocare gli altri numeri utilizzando lo stesso metodo usato per il numero 5.

Facendo ciò si determinano tutte le tavole di Young di forma $[2, 2]$ e quelle di forma $[3, 1]$ e si otterrà:

1	3	4
2	5	

1	2	4
3	5	

1	2	3
4	5	

1	3	5
2	4	

1	2	5
3	4	

1.3 La funzione di partizione

La **funzione di partizione** indica il numero di partizioni per un intero positivo n .

Esempio 1.8. Sia 4 l'intero positivo preso in esame, le sue possibili partizioni sono

$$4 = 1 + 1 + 1 + 1$$

$$4 = 2 + 1 + 1$$

$$4 = 2 + 2$$

$$4 = 3 + 1$$

$$4 = 4$$

e indicando con $p(n)$ il numero di partizioni di n , in questo caso si ha che $p(4) = 5$.

La funzione di partizione non è né moltiplicativa e né additiva cioè non valgono le seguenti uguaglianze:

$$p(n \cdot m) = p(n) \cdot p(m)$$

e

$$p(n + m) = p(n) + p(m)$$

per ogni n, m interi positivi.

I primi valori della funzione di partizione $p(n)$, partendo da 0 sono:

$$1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, \dots$$

La seguente curva rappresenta l'andamento della funzione di partizione

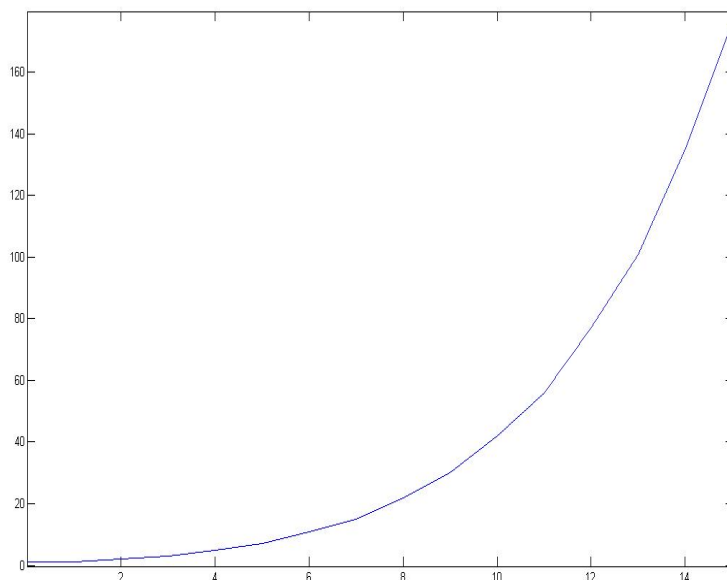


Figura 1.1: Curva della funzione di partizione

dove l'asse delle ascisse rappresenta i valori degli interi positivi presi in esame, mentre l'asse delle ordinate rappresenta i valori possibili che assume la funzione di partizione.

In particolare, sono stati calcolati per i primi 15 interi positivi i corrispondenti valori della funzione di partizione. Si può subito notare che la funzione di partizione al crescere di n cresce molto in fretta, in forma esponenziale.

Il problema di trovare il valore della funzione di partizione può essere inteso in vari modi: infatti, in base a come vengono considerati gli oggetti e/o le parti in cui si raggruppano tali oggetti, si ottengono diverse questioni.

Per esempio, il problema può essere quello di partizionare, cioè: n oggetti indistinguibili in parti indistinguibili (questo è il caso che tratterò); n oggetti distinguibili in parti indistinguibili; n oggetti indistinguibili in parti distinguibili; n oggetti distinguibili in parti distinguibili; n oggetti distinguibili in un numero fissato m di parti indistinguibili; etc. . . .

In altri termini, si tratta di contare le partizioni di un dato insieme finito X distinguendone gli elementi che costituiscono i vari blocchi. Esistono diversi metodi per calcolare la funzione $p(n)$.

Dal punto di vista combinatorio è interessante l'utilizzo di una funzione ausiliaria $p'(n, m)$, che conta il numero di partizioni di n in cui l'addendo maggiore

vale m .

Nell' *Esempio* 1.8 si è calcolata la partizione di 4 e utilizzando la funzione ausiliaria p' si può osservare che:

$$p'(4, 1) = 1, \quad p'(4, 2) = 2, \quad p'(4, 3) = 1, \quad p'(4, 4) = 1$$

e si può notare che:

$$p(4) = 5 = 1 + 2 + 1 + 1 = p'(4, 1) + p'(4, 2) + p'(4, 3) + p'(4, 4).$$

Voglio calcolare una funzione ricorsiva che identifichi il valore di $p(n)$ per ogni n , cioè voglio definire $p'(n, m)$ dove $0 \leq m \leq n$. Poiché, per definizione della funzione $p'(n, m)$, esiste almeno un addendo con valore m , manca da calcolare la parte $(n - m)$, tenendo conto che non si dovranno considerare le partizioni di $n - m$ con addendi maggiori di m .

Da ciò segue che non dovrò più calcolare il valore di $p'(n, m)$, ma quello di $p'(n - m, k)$ con $0 \leq k \leq m$. Quindi, ho trovato che:

$$p(n) = \sum_{m=1}^n p'(n, m) \quad (1.11)$$

$$p'(n, m) = \sum_{k=1}^m p'(n - m, k) \quad (1.12)$$

dove (1.11) rappresenta il fatto che $p(n)$ è data dalla sommatoria dei $p'(n, m)$, mentre (1.12) definisce ricorsivamente il valore della funzione ausiliaria p' , utilizzando il ragionamento fatto prima.

Nella seguente tabella sono stati riportati i valori della funzione p' al variare dei due argomenti n e m .

																1													
																1	1												
															1	1	2												
														1	1	2	3												
														1	1	2	3	5											
														1	1	2	3	5	7										
														1	1	2	3	5	7	11									
														1	1	2	3	5	7	11	15								
														1	1	2	3	5	7	11	15	22							
														1	1	2	3	5	7	11	15	22	29						
														1	1	2	3	5	7	11	15	21	28	38					
														1	1	2	3	5	7	11	14	20	26	35	44				
														1	1	2	3	5	7	10	13	18	23	30	37	47			
														1	1	2	3	5	6	9	11	15	18	23	27	34	39		
														1	1	2	3	4	5	7	8	10	12	14	16	19	21	24	
														1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8
														1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
																	n												

Nell'asse orizzontale sono rappresentati i valori di n , mentre nell'asse verticale quelli di m . Le caselle vuote rappresentano il valore nullo.

Considerando la definizione (1.11), per calcolare $p(n)$ basta sommare i valori dell' n -esima colonna, mentre il valore nelle coordinate (n, m) si calcola sommando gli elementi (avente ordinata minore o uguale a m) nella $(n-m)$ -esima colonna. Analizzando la tabella, partendo dalle righe più in basso e lette da sinistra, si può osservare che:

- Le righe, considerate partendo da quella più in basso e lette da sinistra cominciano da punti diversi, ma convergono all'aumentare di m ;
- La prima riga dal basso è una sequenza infinita di 1 (questo accade per definizione);
- La seconda riga è la sequenza dei numeri naturali dove ogni termine appare due volte di fila;
- La stessa convergenza si ottiene leggendo le linee dall'alto verso il basso.

Attraverso gli ultimi due punti si ottengono le seguenti proprietà:

$\forall n \exists r_0$ tale che, $\forall r \geq r_0$, valgono

$$p(n) = p'(n + r, n) \quad (1.13)$$

$$p(n) = p'(r, r - n). \quad (1.14)$$

La proprietà (1.13) si dimostra considerando la definizione di $p'(n+r, n)$: il calcolo del valore della casella di coordinate $(n+r, n)$ andrà a sommare i valori della colonna n -esima di ordinate minori di r . Invece, se $r > n$, in tale somma finiranno tutti i valori positivi. Trovando $r_0 = n$ si è dimostrata la proprietà (1.13).

Osservando gli elementi sulla bisettrice del triangolo raffigurato in tabella, si può ottenere un'altra proprietà che deriva dal fatto che questi elementi coincidono con i termini della successione di partizione:

$$p(n) = p'(2n+1, n). \quad (1.15)$$

La dimostrazione di questa proprietà viene ricavata dalla relazione (1.11) ponendo $r = n + 1$.

1.4 Partizioni ordinate

Considero un intero positivo, per esempio, 4 ed elenco tutti i modi possibili di scrivere questo numero come somma di interi positivi:

a) $4 = 4$

b) $4 = 3+1$

c) $4 = 2+2$

d) $4 = 2+1+1$

e) $4 = 1+1+1+1$

Ho, così, ottenuto 5 modi di scrivere 4. Si può osservare che i punti $b)$ e $d)$ si possono scrivere in altri modi: cioè il punto $b)$ può essere scritto anche nel seguente modo

$$4 = 1 + 3$$

mentre il punto $d)$ è equivalente alle seguenti somme

$$4 = 1 + 1 + 2 \text{ e } 4 = 1 + 2 + 1.$$

Quindi se si tiene conto dell'ordine degli addendi, l'intero positivo 4 si può scrivere come somma di interi positivi non in 5 modi, ma in 8 modi.

In generale, tutto questo discorso lo si può rappresentare nel seguente modo:

Sia n un intero positivo e siano $\lambda_1, \lambda_2, \dots, \lambda_m$ interi positivi con

$\lambda_1 > \lambda_2 > \dots > \lambda_m$ tali che $n = \lambda_1 + \lambda_2 + \dots + \lambda_m$ allora il numero di partizioni ordinate di n con gli stessi addendi è dato da

$$\frac{(f_1 + f_2 + \dots + f_m)!}{f_1! f_2! \dots f_m!} \quad (1.16)$$

dove f_i è la frequenza dell' addendo λ_i e m è il numero di addendi.

Esempio 1.9. Consideriamo l'intero 5 e applichiamo (1.16). Troviamo tutti i modi di scrivere 5 come somma di interi positivi.

$$5 = 5$$

questa partizione si può scrivere in un solo modo, infatti:

$$\frac{\lambda_5!}{\lambda_5!} = \frac{1!}{1!} = 1$$

Consideriamo quest'altra partizione:

$$5 = 4 + 1$$

mentre questa la si può scrivere anche in un altro modo, infatti dalla formula (1.16) si ottiene che:

$$\frac{(\lambda_4 + \lambda_1)!}{\lambda_4! \lambda_1!} = \frac{(1+1)!}{1!1!} = 2$$

Quindi:

$$5 = 4 + 1$$

e

$$5 = 1 + 4$$

Si avrà così che anche

$$5 = 3 + 2$$

che si scriverà anche in un altro modo e cioè

$$5 = 2 + 3$$

e non esiste un altro modo perchè dalla formula (1.16) si ottiene che il numero 5 come somma dei numeri 2 e 3 lo si può scrivere solo in due modi. Consideriamo ora

$$5 = 3 + 1 + 1$$

e attraverso (1.16) calcoliamo il numero di modi in cui si può scrivere 5 come somma di 3, 1 e 1.

$$\frac{(\lambda_3 + \lambda_1)!}{\lambda_3! \lambda_1!} = \frac{(1+2)!}{1!2!} = 3$$

e questi tre modi sono:

$$5 = 3 + 1 + 1$$

$$5 = 1 + 3 + 1$$

$$5 = 1 + 1 + 3$$

L'intero 5 lo si può anche scrivere così

$$5 = 2 + 1 + 1 + 1$$

e dalla (1.16) si ottiene

$$\frac{(\lambda_2 + \lambda_1)!}{\lambda_2! \lambda_1!} = \frac{(1+3)!}{1!3!} = 4$$

esistono, cioè, quattro modi per scrivere 5 come somma di 2 e 1:

$$5 = 2 + 1 + 1 + 1$$

$$5 = 1 + 2 + 1 + 1$$

$$5 = 1 + 1 + 2 + 1$$

$$5 = 1 + 1 + 1 + 2$$

Si consideri ora 5 come somma di soli 1

$$5 = 1 + 1 + 1 + 1 + 1$$

e si applichi la formula (1.16)

$$\frac{(\lambda_1)!}{\lambda_1!} = \frac{5!}{5!} = 1$$

e cioè esiste un solo modo.

Infine consideriamo 5 come somma di 2 e 1 e applichiamo la formula (1.16)

$$\frac{(\lambda_2 + \lambda_1)!}{\lambda_2! \lambda_1!} = \frac{(2+1)!}{2!1!} = 3$$

Otteniamo che si può scrivere in 3 modi che sono i seguenti:

$$5 = 1 + 2 + 2$$

$$5 = 2 + 1 + 2$$

$$5 = 2 + 2 + 1$$

In conclusione, abbiamo trovato che l'intero positivo 5 si può scrivere come somma ordinata di interi positivi in 16 modi e non solo in 7 modi come si era trovato nel paragrafo precedente.

Consideriamo la seguente tabella

n	1	2	3	4	5	6	7	8	...	n
$P(n)$	1	2	3	5	7	11	15	22	...	
$P_\sigma(n)$	1	2	4	8	16	32	64	128	...	2^{n-1}

e si può subito notare la differenza dei risultati ottenuti per ogni intero positivo utilizzando due metodi distinti: nella riga in corrispondenza di $P(n)$ viene utilizzato il metodo definito nei precedenti paragrafi e generalizza la curva (1.1), mentre nella riga in corrispondenza di $P_\sigma(n)$ sono stati riportati i risultati ottenuti dalla (1.16).

Si può notare che i valori di $P_\sigma(n)$ al variare di n sono potenze di 2, infatti:

$$P_\sigma(1) = 1 = 2^0 = 2^{1-1}$$

$$P_\sigma(2) = 2 = 2^1 = 2^{2-1}$$

$$P_\sigma(3) = 4 = 2^2 = 2^{3-1}$$

.

.

.

Utilizzando il *teorema del binomio* si ha che $\forall n P_\sigma(n) = 2^{n-1}$, infatti:

$$\sum_{k=0}^{n-1} \binom{n-1}{k} = \sum_{k=1}^n \binom{n}{k-1} 1^{k-1} 1^{n-k+1} = (1+1)^{n-1} = 2^{n-1} \quad (1.17)$$

dove k è il numero degli addendi, $\binom{n-1}{k}$ è il numero di modi possibili di scrivere n come somma di $k+1$ addendi.

Capitolo 2

Storia

Questo capitolo tratta di come si è affrontata la teoria delle partizioni nel tempo.

Nel diciottesimo secolo Eulero riuscì a trovare un metodo di calcolo lento, complesso e inapplicabile a numeri abbastanza grandi (si è fatto riferimento a [4]). Nel ventesimo secolo Ramanujan e Hardy riuscirono a trovare una formula efficiente per numeri inferiori a 200, ma poiché nella formula è presente il numero π da essa si ricavano valori approssimativi e con un numero infinito di decimali (si è fatto riferimento a [1]).

Nel 1937 Hans Rademacher migliorò la formula di Ramanujan, elaborando una serie convergente che tende a $p(n)$ (si è fatto riferimento a [6]).

Nel gennaio 2011 Ken Ono estese la formula di Ramanujan e trovò che i numeri di partizione hanno comportamento "frattale" e riuscì ad ottenere una formula che permette di calcolare le partizioni di qualsiasi intero attraverso una somma di numeri finiti (si è fatto riferimento a [8] ed a [9]).

2.1 Eulero e le infinite partizioni

Come si è visto nel primo capitolo, la teoria delle partizioni si occupa di determinare in quanti modi possibili un numero possa essere scritto come somma di interi positivi; nasce, così, il problema di trovare una relazione tra un numero e la sua partizione, ma ciò non è semplice.

Inizio ora a calcolare le partizioni di alcuni numeri e cerco di capire se esiste effettivamente una relazione:

$$p(1) = 1$$

$$p(2) = 2$$

$$p(3) = 3$$

$$p(4) = 5$$

$$p(5) = 7$$

Come si può notare fino al numero 3 il rapporto tra il numero e il numero delle sue partizioni è uno-a-uno, mentre dal 4 in poi non si ha più questa relazione. Quindi, si può concludere che non esiste una relazione semplice tra il numero e il numero delle sue partizioni. Per numeri abbastanza piccoli è semplice calcolare in quanti modi si può scrivere, ma per numeri come 100, 1000, ecc. possono nascere difficoltà e in più ci si impiega troppo tempo (crescita esponenziale, NP).

Viene così da chiedersi: come si può determinare il valore della funzione p senza calcolarla effettivamente?

Nel diciottesimo secolo Leonhard Euler (Eulero), matematico e fisico svizzero, nato a Basilea nel 1707 e morto nel 1783 a San Pietroburgo, attraverso una funzione generatrice contribuì alla teoria delle partizioni.

Questa funzione fu così definita:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\dots} \quad (2.1)$$

Questa espressione definisce un rapporto tra 1 e un prodotto infinito che lo si può identificare con la seguente espressione

$$\prod_{i=1}^{\infty} (1-x^i) \quad (2.2)$$

quindi risulta essere un quoziente infinito. La funzione $p(n)$, infatti, per come è stata definita, deve essere calcolata per ognuno degli infiniti numeri naturali. Ora calcolo (2.2):

$$\prod_{i=1}^{\infty} (1-x^i) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} \dots$$

Sostituisco un 1 al posto di ognuna di queste potenze di x che sono rimaste nel prodotto e metto uno 0 al posto di ogni termine mancante e ottengo la seguente rappresentazione:

$$1 - 1 - 1 + 0 + 0 + 1 + 0 + 1 + 0 + 0 + 0 + 0 - 1 + 0 \dots \quad (2.3)$$

Fatto ciò posso dividere 1 per (2.3):

1	0	0	0	0	0	0	0	...	1	-1	-1	0	0	1	0
1	-1	-1	0	0	1	0	0	...	1	1	2	3	5	7	11
	1	1	0	0	-1	0	0	...							
	1	-1	-1	0	0	1	0	...							
		2	1	0	-1	-1	0	...							
		2	-2	-2	0	0	0	...							
			3	2	-1	-1	0	...							
			3	-3	-3	0	0	...							
				5	2	-1	0	...							
				5	-5	-5	0	...							
					7	4	0	...							
					7	-7	0	...							
						11	0	...							

Si può osservare che ai numeri presenti nel risultato corrispondono in ordine i numeri delle partizioni per ognuno dei primi numeri naturali.

2.2 Ramanujan e Hardy

Srinivasa Aiyangar Ramanujan (nato a Erode, 22 dicembre 1887 e morto a Chennai, 26 aprile 1920) fu un matematico indiano che si occupò principalmente della teoria analitica dei numeri e una sua caratteristica era quella di enunciare formule senza dimostrazioni. Assieme ad Hardy riuscì a trovare una formula che esprimesse la successione dei numeri di partizione.

Quest'ultimo, Godfrey Harold Hardy (nato a Cranleigh, 7 febbraio 1877 e morto a Cambridge, 1 dicembre 1947), fu anche esso un noto matematico britannico e preferiva che il suo lavoro fosse considerato matematica pura, forse a causa del suo odio per la guerra e gli usi militari a cui la matematica era stata applicata.

Nel 1914 Ramanujan arrivò a Cambridge e da qui iniziò una delle più grandi collaborazioni della storia della matematica. La coppia Hardy-Ramanujan fece pensare a una squadra in cui era presente un pò di buono e un pò di

cattivo: il buono è l'ottimista pieno di proposte folli, mentre il cattivo è il pessimista. Ramanujan aveva bisogno che Hardy, il critico, tenesse a bada il suo entusiasmo mentre interrogavano le loro idee matematiche.

Tra Ramanujan e Hardy c'era un contrasto culturale. Infatti, Hardy e Littlewood (noto matematico britannico) che pretendevano dimostrazioni rigorose, non riuscivano a capire da dove venissero le idee di Ramanujan, il loro nuovo collega. Ramanujan sosteneva che le idee gli venivano portate in sogno dalla dea Namagiri, protettrice della sua famiglia. Alcuni del suo villaggio credevano che fosse portatrice di demoni, mentre per Ramanujan era la spiegazione dei lampi di illuminazione sul campo matematico.

Ramanujan era passato dall'isolamento matematico dell'India alla solitudine culturale di Cambridge, ma fortunatamente aveva trovato un compagno con il quale poteva affrontare il mondo matematico. Ramanujan riusciva a trovare conforto solo quando entrava nello studio di Hardy e quando si rifugiava nelle sue formule e nelle sue equazioni.

Hardy capì che educare Ramanujan era un'impresa di equilibrismo: aveva paura che se avesse costretto Ramanujan a dimostrare le sue idee avrebbe potuto distruggere la sua fiducia in se stesso o spezzare l'incantesimo della sua ispirazione. Littlewood ebbe il compito di educare Ramanujan cioè di farlo famigliarizzare con il rigore della matematica occidentale, ma fu un compito impossibile.

Hardy e Ramanujan, comunque, continuarono nella loro ricerca delle proprietà dei numeri primi. Queste idee divennero un primo passo alla dimostrazione della congettura di Goldbach (cioè ogni numero pari è la somma di due numeri primi).

In una lettera Ramanujan scrisse di aver trovato una formula che esprime la sequenza dei numeri primi e di essere riuscito a capire come generare un'altra sequenza cioè quella delle partizioni di un numero intero. I matematici di quel tempo pensavano che esistesse solo una formula in grado di produrre una stima che non discostasse molto dall'effettivo numero di partizioni di N . Ma a Ramanujan non era mai stato insegnato se temere questi generi di sequenze, così volle trovare una formula che identificasse proprio il numero di modi possibili per suddividere un qualsiasi numero intero.

Attraverso la collaborazione di Hardy, Ramanujan riuscì a trovarne una:

$$p(n) = \frac{1}{2\pi\sqrt{2}} \sum_{k < \alpha\sqrt{n}} A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{e^{\frac{c\lambda_n}{k}}}{\lambda_n} \right) + O\left(n^{-\frac{1}{4}}\right) \quad (2.4)$$

con

$$c = \pi \sqrt{\frac{2}{3}},$$

$$\lambda_n = \sqrt{n - \frac{1}{24}}$$

e

$$A_k(n) = \sum_{h(\bmod k)} \omega_{h,k} e^{\frac{-2\pi i h n}{k}}$$

dove $\omega_{h,k} = e^{\pi i s(h,k)}$ in cui

$$s(h, k) := \sum_{\mu=1}^k \left(\left(\frac{h\mu}{k} \right) \left(\frac{\mu}{k} \right) \right)$$

con $k \geq 1$ e $(h, k) = 1$.

L'espressione (2.4) è una serie asintotica, con $n \rightarrow \infty$ e con α costante positiva, e non fornisce il numero esatto di partizioni, ma solo una risposta che è corretta se la si approssima al numero intero più vicino. Per esempio, sostituendo il numero 200 si ottiene un valore non intero approssimato a 3972999029338.

Ramanujan non riuscì a trovare una formula che desse un esatto numero di partizioni di un intero, tuttavia questo risultato fu comunque importante negli innumerevoli tentativi di dimostrazione della congettura di Goldbach.

Il lavoro svolto da Hardy e Ramanujan prese il nome di *Metodo del cerchio di Hardy e Littlewood* dove la parola *cerchio* deriva dai piccoli diagrammi presenti nei calcoli di Hardy e Ramanujan e rappresentavano cerchi nella mappa dei numeri immaginari attorno ai quali i due matematici cercavano di eseguire integrazioni. Questo metodo viene attribuito ad Hardy e a Littlewood, invece, che ad Hardy e a Ramanujan perché Littlewood e Hardy lo usarono per cercare di dimostrare la congettura di Goldbach. Anche se non riuscirono a dimostrare che ogni numero pari poteva essere espresso come somma di due numeri primi, nel 1923 Hardy e Littlewood dimostrarono che tutti i numeri pari maggiori di un certo numero fissato potevano essere scritti come somma di numeri primi. Affinché la dimostrazione di ciò fosse stata valida, l'ipotesi di Riemann doveva essere vera.

In seguito, nel 1910 Ramanujan, impaziente che le sue idee venissero riconosciute, scoprì quanto fossero importanti i numeri primi per la matematica e, poiché credeva che tutta la matematica e le sue strutture si potessero esprimere con precisione attraverso formule o equazioni, non abbandonò l'idea che esistesse una formula che producesse i numeri primi. Affermò che

$$1 + 2 + 3 + \dots + \infty = -\frac{1}{12} \quad (2.5)$$

Questa uguaglianza arrivò ad Hardy e a Littlewood che rimasero stupiti, ma poco dopo riuscirono a capire che era un nuovo metodo per definire la parte

mancante del "paesaggio zeta" di Riemann cioè era la soluzione di Riemann per il calcolo della funzione zeta quando si inseriva il numero -1 . Era così un perfezionamento della formula di Gauss per il conteggio dei numeri primi introdotto da Riemann.

2.3 Hans Rademacher

Forse il teorema più famoso di Rademacher (nato il 3 aprile 1882, Wand-sbeck, ora Hamburg-Wandsbeck e morto il 7 febbraio 1969 a Haverford, Pennsylvania, USA) è quello riguardante la formula esatta della funzione di partizione $p(n)$. Posto $c = \pi\sqrt{\frac{2}{3}}$ e $\lambda_n = \sqrt{n^{-\frac{1}{24}}}$, Rademacher provò che

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{\sinh\left(\frac{c\lambda_n}{k}\right)}{\lambda_n} \right) \quad (2.6)$$

dove

$$A_k(n) = \sum_{h \pmod{k}} \omega_{h,k} e^{-\frac{2\pi hn}{k}}$$

con $(h, k) = 1$ e con $\omega_{h,k} = e^{\pi i sh, k}$.

La storia di questa formula è molto interessante.

Nel 1917 Hardy e Ramanujan, introducendo il loro famoso metodo del cerchio, avevano meravigliato la comunità matematica trovando una serie asintotica per $p(n)$, cioè :

$$p(n) = \frac{1}{2\pi\sqrt{2}} \sum_{k < \alpha\sqrt{n}} A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{e^{\frac{c\lambda_n}{k}}}{\lambda_n} \right) + O\left(n^{-\frac{1}{4}}\right) \quad (2.7)$$

per n che tende a ∞ , dove α è una costante positiva.

Hanno iniziato col definire una funzione generatrice nel seguente modo

$$f(x) := \prod_{n=1}^{\infty} (1 - x^n)^{-1} \quad (2.8)$$

per $p(n)$. Poi, hanno approssimato f tramite una funzione F e hanno integrato $f - F$ sotto la dissezione del cerchio tramite le serie, o più precisamente, successione di Farey di ordine N , cioè tramite le successioni di tutte le frazioni ai minimi termini con i denominatori che non superano N . Infine, hanno trovato una relazione tra i parametri n e N , cioè $N = \alpha\sqrt{n}$.

Nel 1936 durante la preparazione delle lezioni per il corso di laurea in teoria

dei numeri analitica presso l'Università di Pennsylvania, Hans Rademacher applicò, alla formula trovata da Ramanujan, la formula di trasformazione di Dedekind

$$\eta(\tau) = \frac{e^{\frac{\pi i \tau}{12}}}{f(e^{2\pi i \tau})}$$

per ottenere il termine principale e variando n e N . Rademacher trovò così che

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^N A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{\sinh\left(\frac{e\lambda_n}{k}\right)}{\lambda_n} \right) + O\left(N^{-\frac{1}{2}} e^{2\pi n N^{-2}}\right) \quad (2.9)$$

per $N \rightarrow \infty$. Si può osservare che i termini principali sono indipendenti da N . Fissato n e tendendo N a ∞ , si ottiene così l'espressione (2.6).

Si noti che gli addendi in (2.6) differiscono da quelli in (2.7). Quando Rademacher, infatti, concluse che l'espressione (2.6) rappresenta la funzione $p(n)$, pensò che avesse fatto degli errori di calcolo, ma il giorno seguente dopo una accurata analisi ai suoi calcoli, scoprì che (2.6) era effettivamente corretta. Più tardi, Lehmer, matematico americano, provò che la somma in (2.7), estendendola all'infinito diverge.

I numeri $A_k(n)$ compaiono sia nelle formule di Hardy e Ramanujan che in quelle di Rademacher e Lehmer trovò che questi numeri godono di alcune proprietà notevoli sulle fattorizzazioni.

Utilizzando i loro teoremi sulle congruenze per somme di Dedekind, Rademacher e Whiteman, matematico americano, diedero semplici dimostrazioni di questi teoremi di fattorizzazione. Successivamente, Selberg, matematico norvegese, scoprì una formula più semplice per $A_k(n)$, cioè,

$$A_k(n) = \sqrt{\frac{k}{3}} \sum_{\substack{(3j^2+j) \equiv -n \\ \pmod{k}}} (-1)^j \cos\left(\frac{\pi(6j+1)}{6k}\right). \quad (2.10)$$

Dopo che Whiteman diede una prima pubblicazione della dimostrazione di (2.10), Rademacher ideò una semplice prova di (2.10) in funzione della formula di trasformazione di $\eta(n)$.

2.4 Ken Ono e i frattali

Ken Ono (nato in Filadelfia il 20 marzo 1968) è un matematico statunitense specializzato in teoria dei numeri e ha trovato una nuova teoria sulla partizione di un numero intero.

Per mesi Ono e il suo gruppo di ricerca hanno studiato quel problema, senza avere nessun risultato, ma nel settembre del 2010, durante un'escursione alle cascate Tallulah in Georgia, Ono e Zachary Kent osservarono la struttura dei gruppi di alberi e iniziarono a pensare come se potessero camminare attraverso le partizioni dei numeri. Ono disse che:

”Eravamo in cima delle enormi rocce dove potevamo vedere tutta la valle ed ascoltare il rumore delle cascate, quando abbiamo realizzato che le partizioni dei numeri sono frattali, ed entrambi abbiamo iniziato a ridere.”

Benoit Mandelbrot (1924-2010, matematico polacco) inventò il termine frattale nel 1980 per identificare tutto quello che sembra irregolare nella geometria delle forme naturali.

Più precisamente, è un oggetto geometrico che si ripete nella struttura allo stesso modo su scale diverse, cioè che non cambia aspetto anche se visto attraverso una lente di ingrandimento.

Con questa camminata Ono e Kent idearono una nuova teoria da cui nasce una nuova classe di frattali e attraverso questa teoria si possono dimostrare le congruenze di Ramanujan.

Ono e il suo gruppo di ricerca dimostrarono che le proprietà di divisibilità delle partizioni dei numeri sono frattali per ogni numero primo. Ma le osservazioni tratte da questa esperienza non soddisfecero Ono e il suo gruppo e, così, essi cercarono di determinare una formula che potesse rappresentare questa teoria.

Un altro episodio importante si è svolto in un luogo famoso: la ”spaghetti junction”. Mentre Ono e Jan Bruinier erano bloccati nel traffico in un noto incrocio di Atlanta, chiacchierarono in macchina e cercarono di trovare un modo per eliminare l'infinita complessità del metodo di Rademacher: volevano cercare una formula che richiedesse solo un numero finito di numeri. Ono affermò che:

”Abbiamo trovato una funzione, \mathbf{P} , che è una sorta di oracolo magico. Posso prendere qualsiasi numero, inserirlo dentro \mathbf{P} ed istantaneamente calcolare le partizioni di quel numero. \mathbf{P} non dà come risultato un numero terribile con infinite cifre decimali. È quella formula algebrica finita che stavamo tutti cercando.”

Ono, in una sua conferenza, spiega la sua teoria sulle partizioni di un intero positivo utilizzando il concetto di "Yin Yang" : in particolare, enuncia risultati relativi alla successione $p(n)$ ed esprime le sue proprietà.

Introduce la sua scoperta parlando della teoria di Eulero e degli sviluppi nei successivi 150 anni, racconta che si sono calcolate le prime 200 valutazioni applicando questa teoria. A questo punto fa una osservazione: "Nell'universo matematico ciò significa di non essere in grado di vedere oltre Marte". Poi parla della teoria di Hardy e Ramanujan e, a seguire, di quella di Rademacher. Di quest'ultima osserva che è una serie, ma si può ottenere il valore di $p(n)$ facendo un troncamento o un arrotondamento del risultato ottenuto dalla formula di Rademacher.

Nella slide successiva enuncia il seguente teorema:

Teorema 2.4.1. (Brunier-Ono) *Abbiamo trovato una funzione $P(z)$ tale che*

$$p(n) = \frac{1}{24n-1} (P(\alpha_{n,1}) + P(\alpha_{n,2}) + \dots + P(\alpha_{n,h_n})) \quad (2.11)$$

dove $P(\alpha_{n,m})$ sono algebrici, mentre le α sono le radici di $h_n \sim \sqrt{n}$ equazioni quadratiche.

Esempio 2.1. Per $h_1 = 3$ si ha:

$$\begin{aligned} \frac{1}{23} P\left(\frac{-1+\sqrt{-23}}{12}\right) &= \frac{1}{3} + \frac{\beta^{\frac{2}{3}}+127972}{6\beta^{\frac{1}{3}}} \\ \frac{1}{23} P\left(\frac{-13+\sqrt{-23}}{24}\right) &= \frac{1}{3} - \frac{\beta^{\frac{2}{3}}+127972}{12\beta^{\frac{1}{3}}} + \frac{\beta^{\frac{2}{3}}-127972}{4\sqrt{-3}\beta^{\frac{1}{3}}} \\ \frac{1}{23} P\left(\frac{-25+\sqrt{-23}}{36}\right) &= \frac{1}{3} - \frac{\beta^{\frac{2}{3}}+127972}{12\beta^{\frac{1}{3}}} - \frac{\beta^{\frac{2}{3}}-127972}{4\sqrt{-3}\beta^{\frac{1}{3}}} \end{aligned}$$

con $\beta = 16152909 + 18648492\sqrt{69}$.

Quindi:

$$p(1) = 1 = \frac{1}{23} (P(\alpha_1) + P(\alpha_2) + P(\alpha_3))$$

Finita così la parte "Yin" della storia di $p(n)$, passa a quella "Yang" e Ono domanda: "quante volte $p(n)$ è dispari?". Attraverso diverse prove sperimentali afferma che:

- la metà del numero delle partizioni è dispari;
- un terzo del numero delle partizioni è multiplo di 3;

- partendo da 4, ogni quinta partizione è un multiplo di 5.

Dopo aver osservato ciò, enuncia il teorema di Ramanujan:

Teorema 2.4.2. $\forall n \in \mathbb{N}$ si ha

$$\begin{aligned} p(5n + 4) &\text{ è multiplo di } 5 \\ p(7n + 5) &\text{ è multiplo di } 7 \\ p(11n + 6) &\text{ è multiplo di } 11 \end{aligned}$$

Le affermazioni del teorema precedente sono equivalenti rispettivamente alle seguenti:

$$\begin{aligned} p(5n + 4) &\equiv 0 \pmod{5} \\ p(7n + 5) &\equiv 0 \pmod{7} \\ p(11n + 6) &\equiv 0 \pmod{11} \end{aligned}$$

Ono enuncia anche il seguente teorema che è composto da congruenze, chiamate anche *congruenze di Ramanujan* che sono state dimostrate da Ramanujan, Watson (1938) e Atkin (1967)

Teorema 2.4.3. Congruenze di Ramanujan Se $1 \leq \delta_l(m) \leq l^m$ con $24\delta_l(m) \equiv 1 \pmod{l^m}$ allora

$$\begin{aligned} p(5^m n + \delta_5(m)) &\equiv 0 \pmod{5^m}, \\ p(7^m n + \delta_7(m)) &\equiv 0 \pmod{7^{\left(\frac{m+2}{2}\right)}}, \\ p(11^m n + \delta_{11}(m)) &\equiv 0 \pmod{11^m}. \end{aligned}$$

Ken Ono enuncia, anche, tre teoremi relativi alle congruenze:

Teorema 2.4.4. Teorema di Radu $\forall n \in \mathbb{N}$ non esistono forme aritmetiche del tipo $An + B$ tali che

$$p(An + B) \equiv 0 \pmod{2} \tag{2.12}$$

$$p(An + B) \equiv 0 \pmod{3} \tag{2.13}$$

Teorema 2.4.5. Teorema di Ahlgren e Boylan Le coppie (l, a) per le quali

$$p(ln + a) \equiv 0 \pmod{l} \tag{2.14}$$

sono solo le coppie seguenti: $(5, 4)$, $(7, 5)$ e $(11, 6)$.

Teorema 2.4.6. Teorema di Ono $\forall \Omega \geq 5$, con Ω primo, esistono infinite forme $An + B$ tali che

$$p(An + B) \equiv 0 \pmod{\Omega} \quad (2.15)$$

Ha enunciato questi teoremi per dire che la maggior parte dei numeri di partizione non è adatto alle strutture delle congruenze di Ramanujan e così Ono domanda: "Quindi quali proprietà devono avere?". Risponde a questa domanda con il seguente teorema:

Teorema 2.4.7. Teorema di Folsom, Kent e Ono Il numero delle partizioni è frattale $\forall l \geq 5$.

e definisce il termine "frattale" nel modo seguente:

I **frattali** sono strutture complesse infinite con le seguenti due proprietà:

- sono formate da strutture induttive o ricorsive;
- sono più volte simili a se stessi su scale arbitrariamente piccole.

Si ha, quindi, che i valori della funzione $p(n)$ al variare dell'intero n sono simili, si ha una semplice struttura induttiva ed esiste la dimensione di Hausdorff (identificata con $\delta_l(m)$) che è minore o uguale di

$$\frac{l-1}{12} - \frac{l^2-1}{24l}$$

In particolare, la dimensione di Hausdorff è nulla solo per $l = 5, 7$ e 11 .

Conclude la sua conferenza aggiungendo il seguente teorema:

Teorema 2.4.8. Teorema di Atkin, Folsom, Kent e Ono

Se $b_1 \equiv b_2 \pmod{2}$, allora $\forall n$ si ha

$$p\left(\frac{l^{b_2}n + 1}{24}\right) \equiv A(b_1, b_2, m)p\left(\frac{l^{b_1}n + 1}{24}\right) \pmod{l^m} \quad (2.16)$$

e con il seguente esempio:

Esempio 2.2. per $m = 1$

$$p\left(\frac{13^{2k+1}n+1}{24}\right) \equiv 6^k p\left(\frac{13n+1}{24}\right) \pmod{13}$$

in particolare per $k = 1$

$$p(13n^3 + 1007) \equiv 6p(13n + 6) \pmod{13}$$

Si trova che

$$6 \sum_{n=0}^{\infty} p(13n+6)q^n = 66 + 2940q + 50094q^2 + \dots \equiv 1 + 2q + 5q^2 + 10q^3 + 7q^4 + 10q^5 \pmod{13}$$

e

$$\sum_{n=0}^{\infty} p(13^2n + 1007)q^n \equiv 1 + 2q + 5q^2 + 10q^3 + 7q^4 + 10q^5 \pmod{13}$$

per $n = 0, 1$ e 2

$$45p(13^2 \cdot 0 + 162) \equiv 99 \pmod{13^2}$$

$$45p(13^2 \cdot 1 + 162) \equiv 89 \pmod{13^2}$$

$$45p(13^2 \cdot 2 + 162) \equiv 20 \pmod{13^2}$$

mentre per numeri grandi:

$$p(13^4 \cdot 0 + 27371) \equiv 99 \pmod{13^2}$$

$$p(13^4 \cdot 1 + 27371) \equiv 89 \pmod{13^2}$$

$$p(13^4 \cdot 2 + 27371) \equiv 20 \pmod{13^2}$$

Capitolo 3

Applicazioni

Nel seguente capitolo tratto di due applicazioni elementari, ma, allo stesso tempo, molto importanti: le classi di coniugio nel gruppo simmetrico S_n ([5] e [3]) e le classificazioni dei gruppi abeliani di ordine p^n , con p primo ([2]).

3.1 Le classi di coniugio nel gruppo simmetrico S_n

Questo paragrafo si suddivide in due parti: nella prima parte introduco alcune nozioni fondamentali dei gruppi e del coniugio di un gruppo; nella seconda parte affronto l'argomento principale di questo paragrafo definendo prima un particolare gruppo, cioè quello delle permutazioni, e poi descrivo le sue classi di coniugio.

3.1.1 I gruppi e il coniugio

Definizione 3.1. Un *gruppo* è un insieme G con una operazione

$$G \times G \rightarrow G$$
$$(a, b) \mapsto ab \text{ (oppure } a \cdot b)$$

e un elemento $1 \in G$, chiamato *identità*, tale che valgono le seguenti proprietà:

a) siano a, b e c tre elementi di G . Allora

$$a(bc) = (ab)c \tag{3.1}$$

cioè l'operazione \cdot gode della *proprietà associativa*;

b) se $a \in G$ allora

$$1 \cdot a = a \cdot 1 = a \quad (3.2)$$

in particolare 1 viene chiamato *elemento neutro*;

c) $\forall a \in G \exists a^{-1} \in G$ con

$$aa^{-1} = a^{-1}a = 1 \quad (3.3)$$

e questo si traduce nel fatto che ogni elemento ha un inverso.

Esempio 3.1. Sia X un insieme qualsiasi e considero $S(X)$, cioè considero l'insieme delle permutazioni di X ovvero:

$$S(X) := \{f | f : X \rightarrow X \text{ biunivoca}\}$$

Se $f, g \in S(X)$ e denoto con $fg = f \circ g$ la composizione di g e di f , cioè la funzione biunivoca si definisce nel seguente modo:

$$(fg)(x) = f(g(x))$$

$\forall x \in X$. Si verifica facilmente che vale la proprietà associativa (3.1).

Considero la funzione identica che manda ogni elemento di X in se stesso, questa funzione è l'identità, cioè $1 \in S(X)$, ovvero viene verificata anche la proprietà (3.2). Infine, affinché $S(X)$ sia un gruppo manca da verificare la proprietà (3.3):

$$f \circ f' = f' \circ f = 1$$

$\forall f \in S(X)$, ma poiché $f \in S(X)$, cioè f è biunivoca, allora f è invertibile e quindi esiste $f' = f^{-1}$, cioè esiste una funzione inversa di f .

Si è così dimostrato che $S(X)$ è un gruppo, chiamato il *gruppo delle permutazioni di X* .

Com'è ben noto, in ogni gruppo c'è un unico elemento neutro, ogni elemento ha un solo inverso e inoltre valgono le leggi di cancellazione a destra e a sinistra.

Definizione 3.2. Un gruppo $(G, *)$ si dice *abeliano* se $\forall a, b \in G$ vale che $a * b = b * a$.

Definendo a^m con $m \in \mathbb{Z}$ nel seguente modo:

$$a^m := \begin{cases} \underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_{m \text{ volte}} & \text{se } m > 0 \\ 1 & \text{se } m = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{m \text{ volte}} & \text{se } m < 0 \end{cases}$$

allora valgono le comuni proprietà delle potenze:

- a) $a^{m+n} = a^m a^n$;
- b) $a^{mn} = (a^m)^n$;
- c) $a^{-m} = (a^m)^{-1}$;
- d) se a e $b \in G$ commutano allora $(ab)^m = a^m b^m$.

Definizione 3.3. Due elementi x e y di un gruppo G si dicono *coniugati* se $\exists g \in G$ tali che

$$y = g^{-1} x g$$

e, in particolare, si dice che y è *coniugato* a x mediante g .

La relazione tra gli elementi di G così definita:

$$x \sim y \text{ se esiste } g \in G \text{ tali che } y = g^{-1} x g$$

è di equivalenza. Questa relazione di equivalenza si chiama *coniugio* e le classi di questa relazione vengono chiamate *classi di coniugio*.

Da questa definizione segue che: due elementi si dicono *coniugati* se appartengono alla stessa classe di coniugio.

Teorema 3.1.1. Due elementi x e y di un gruppo G sono coniugati se e solo se esistono due elementi a e b tali che

$$x = ab \text{ e } y = ba$$

Dimostrazione. La condizione è sufficiente perchè

$$ba = a^{-1}(ab)a.$$

Mentre per verificare la necessità basta porre $g = a$ e $g^{-1}x = b$ e sostituire ciò in $y = g^{-1}xg$. \square

Introduciamo la nozione di ordine di un gruppo che servirà per definire la relazione presente tra due elementi coniugati e il loro ordine.

Definizione 3.4. Sia G un gruppo finito, l'ordine di G , denotato con $|G|$, è il numero degli elementi di G . Sia G un gruppo e sia a un suo elemento, se $a^k \neq 1 \forall k \neq 0$ allora si dice che a ha *ordine infinito*, mentre se esiste un $k \neq 0$ tali che $a^k = 1$, si chiama *ordine* di a il minimo intero positivo m tale che $a^m = 1$.

Osservazione 1. Un elemento di un gruppo finito ha sempre ordine finito. Infatti se G è finito e $a \in G$, l'insieme $\{a^k \mid k \in \mathbb{Z}\} \subset G$ è finito, perciò $\exists k, l \in \mathbb{Z}$ con $k \neq l$, $a^k \neq a^l$. si ha allora $k - l \neq 0$, $a^{k-l} = a^k (a^l)^{-1} = 1$.

Consideriamo, ora, un gruppo G e un suo elemento a , esiste una funzione $C_a : G \rightarrow G$ tali che $C_a(x) = axa^{-1}$ e si verifica facilmente che questa funzione è un isomorfismo di gruppi.

Sapendo che un isomorfismo di gruppi porta elementi di un dato ordine in elementi dello stesso ordine, segue la seguente proposizione:

Proposizione 3.1.2. *Due elementi coniugati hanno lo stesso ordine.*

3.1.2 I gruppi di permutazioni e il coniugio

Si considera X un insieme con n elementi, $n > 0$, allora si ha che $S(X)$ ha $n!$ elementi.

Definizione 3.5. Per ogni intero positivo n il *gruppo simmetrico* su n lettere è

$$S_n = S(\{1, 2, \dots, n\}).$$

Definizione 3.6. Sia i_1, i_2, \dots, i_l una successione di l elementi di $\{1, 2, \dots, n\}$ tutti distinti con $2 \leq l \leq n$. La permutazione $\gamma \in S_n$ definita da $\gamma(i_k) = i_{k+1}$ per $k = 1, \dots, l-1$, $\gamma(i_l) = i_1, \gamma(j) = j$ se $j \notin \{i_1, \dots, i_l\}$ è detta un *ciclo* di lunghezza l e viene denotato con (i_1, \dots, i_l) .

Esempio 3.2. Considero il gruppo simmetrico S_3 , ha $3!(= 2 \cdot 3 = 6)$ elementi che sono:

$$S_3 = \{id, (13), (12), (23), (123), (132)\}$$

dove con id viene identificata l'identità e cioè

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Proposizione 3.1.3. *Un ciclo si scrive in maniera unica come $\gamma = (i_1 \dots i_l)$, dove $i_1 < i_k$ per $k = 2, \dots, l$.*

Definizione 3.7. Due cicli $(i_1 \dots i_l)$ e $(j_1 \dots j_h)$ si dicono *disgiunti* se $\{i_1, \dots, i_l\}$ e $\{j_1, \dots, j_h\}$ sono insiemi disgiunti.

Teorema 3.1.4. *Ogni permutazione $\alpha \in S_n$, $\alpha \neq id$, si può scrivere come $\alpha = \gamma_1 \dots \gamma_r$, dove i fattori sono cicli tali che γ_i è disgiunto da γ_j se $i \neq j$. Inoltre se $\alpha = \gamma_1 \dots \gamma_r = \delta_1 \dots \delta_s$ sono due rappresentazioni di α come prodotto di cicli a due a due disgiunti, allora $r = s$ ed è possibile riordinare i $\delta_1 \dots \delta_s$ in maniera tale che $\gamma_1 = \delta_1, \dots, \gamma_r = \delta_r$.*

Esempio 3.3. In S_7 considero un suo elemento

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 3 & 7 & 6 \end{pmatrix}$$

e per il teorema precedente posso scrivere α come composizione di cicli disgiunti:

$$\alpha = (1\ 2\ 4)(3\ 5)(6\ 7)$$

Quindi si è visto che una permutazione di S_n è un prodotto di cicli disgiunti e nel paragrafo precedente si è parlato del coniugio. Da tutto ciò segue che una coniugata mediante una permutazione σ è il prodotto dei coniugati di questi cicli mediante σ . Così, il coniugio si riduce al coniugio dei cicli.

Teorema 3.1.5. *Sia $c = (1\ 2 \dots k)$ un ciclo di S_n e sia $\sigma \in S_n$, allora:*

$$(1\ 2 \dots k)^\sigma = (1^\sigma\ 2^\sigma \dots k^\sigma).$$

Dimostrazione. Sia $c_1 = (1^\sigma \ 2^\sigma \ \dots \ k^\sigma)$ e sia $i \in c_1$, $i = j^\sigma$. Si ha:

$$i^{\sigma^{-1}c\sigma} = (j^\sigma)^{\sigma^{-1}c\sigma} = j^{c\sigma} = (j+1)^\sigma = (j^\sigma)^{c_1} = i^{c_1},$$

e dunque $\sigma^{-1}c\sigma$ e c_1 hanno lo stesso valore sugli i che compaiono nel ciclo c_1 . Se $i \notin c_1$, cioè $i \neq j^\sigma \ \forall j = 1, 2, \dots, k$ allora $i^{c_1} = i$,

$$i^{\sigma^{-1}c\sigma} = ((i^{\sigma^{-1}})^c)^\sigma = (i^{\sigma^{-1}})^\sigma = i,$$

e $\sigma^{-1}c\sigma$ e c_1 hanno lo stesso valore anche sugli i che non compaiono nel ciclo c_1 . \square

Attraverso questo teorema si vuole spiegare che il coniugato di un ciclo c mediante una permutazione σ è il ciclo nella cui scrittura compaiono ordinatamente le immagini secondo σ degli elementi di c .

Definizione 3.8. Due elementi $\sigma, \tau \in S_n$ hanno la stessa *struttura ciclica* $[k_1, k_2, \dots, k_n]$ se, quando σ si spezza in k_i cicli di lunghezza i , con $i = 1, 2, \dots, n$, lo stesso accade per τ . Si ha allora:

$$1 \cdot k_1 + 2 \cdot k_2 + \dots + n \cdot k_n = n$$

Per il teorema precedente segue, quindi, che due elementi coniugati hanno la stessa struttura ciclica. Il seguente teorema prova il viceversa:

Teorema 3.1.6. *Se due elementi di S_n hanno la stessa struttura ciclica allora sono coniugati.*

Dimostrazione. Siano

$$\begin{aligned} \sigma &= (i_1 \ i_2 \ \dots \ i_{r_1})(j_1 \ j_2 \ \dots \ j_{r_2}) \dots (k_1 \ k_2 \ \dots \ k_{r_l}), \\ \tau &= (p_1 \ p_2 \ \dots \ p_{r_1})(q_1 \ q_2 \ \dots \ q_{r_2}) \dots (t_1 \ t_2 \ \dots \ t_{r_l}). \end{aligned} \quad (3.4)$$

Considero la seguente permutazione

$$\eta = \begin{pmatrix} i_1 & \dots & i_{r_1} & j_1 & \dots & j_{r_2} & \dots & k_1 & \dots & k_{r_l} \\ p_1 & \dots & p_{r_1} & q_1 & \dots & q_{r_2} & \dots & t_1 & \dots & t_{r_l} \end{pmatrix}$$

questa permutazione porta σ in τ :

$$\eta^{-1}\sigma\eta = \tau.$$

\square

Esempio 3.4. Considero in S_9 le seguenti permutazioni

$$\sigma = (1\ 3)(2\ 4\ 5\ 7)(8\ 9)(6), \quad \tau = (1\ 3)(4\ 6\ 5\ 8)(7\ 9)(2)$$

hanno la stessa struttura ciclica $[1, 2, 0, 1, 0, 0, 0, 0, 0]$ e una η che la coniuga è, per esempio, la seguente

$$\eta = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & 7 & 8 & 9 & 6 \\ 7 & 9 & 4 & 6 & 5 & 8 & 1 & 3 & 2 \end{pmatrix} = (1\ 7\ 8)(2\ 4\ 6)(3\ 9)(5)$$

Avendosi $(1\ 3) = (3\ 1)$, $(7\ 9) = (9\ 7)$ e $(4\ 6\ 5\ 8) = (5\ 8\ 4\ 6)$, allora la seguente permutazione coniuga σ e τ :

$$\eta' = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & 7 & 6 & 8 & 9 \\ 3 & 1 & 5 & 8 & 4 & 6 & 2 & 9 & 7 \end{pmatrix} = (1\ 3)(2\ 5\ 4\ 8\ 9\ 7\ 6).$$

Teorema 3.1.7. *Il numero di elementi di S_n che hanno una data struttura ciclica $(k_1\ k_2\ \dots\ k_n)$, e quindi il numero di elementi di una data classe di coniugio, è*

$$\frac{n!}{1^{k_1} \cdot 2^{k_2} \cdot \dots \cdot n^{k_n} k_1! k_2! \dots k_n!}. \quad (3.5)$$

Dimostrazione. Le cifre $1, 2, \dots, n$ possono comparire in tutti gli $n!$ modi possibili per dar luogo a un prodotto di k_i i -cicli disgiunti, con $i = 1, 2, \dots, n$. Ma data una di queste scritte, la permutazione che ne risulta è la stessa di quelle che si ottengono scambiando tra loro i k_i cicli in tutti i modi possibili, cioè $k_i!$ modi. Inoltre, per ciascun i -ciclo vi sono i scritte e poiché ci sono k_i cicli, vi sono i^{k_i} scritte possibili per gli i -cicli. $\forall i$, la stessa permutazione si ottiene allora i^{k_i} volte, da cui il risultato. \square

Attraverso la seguente proposizione viene definito l'ordine di un elemento di S_n .

Proposizione 3.1.8. *L'ordine di un ciclo di S_n è uguale alla sua lunghezza. L'ordine di una permutazione, α , in S_n è uguale al minimo comune multiplo delle lunghezze di tutti i cicli che intervengono nella scomposizione di α come prodotto di cicli disgiunti.*

Avendo affrontato il discorso sulle partizioni, la proposizione precedente si può enunciare in termini di partizioni di un intero positivo n nel seguente modo:

Proposizione 3.1.9. *Sia $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_r]$ partizione di un intero positivo n tale che*

$$\sum_{i=1}^r \lambda_i = n$$

con $\lambda_i \geq 1$. L'ordine di una permutazione α corrispondente alla partizione λ è il minimo comune multiplo di $\{\lambda_1, \lambda_2, \dots, \lambda_r\}$.

Si vuole ora determinare il numero delle classi di coniugio di S_n . Come si è visto nel primo capitolo, una partizione di un intero positivo n è un insieme di interi positivi $n_1 \leq n_2 \leq \dots \leq n_k$ la cui somma è n . Una classe di coniugio è determinata da una struttura ciclica $[k_1, k_2, \dots, k_n]$, mentre data una tale struttura i $k_i > 0$ danno le molteplicità degli interi i in una partizione di n . Viceversa, data una partizione di n in interi i ciascuno con molteplicità k_i , considerando tutti i prodotti di k_i cicli di lunghezza i , abbiamo, al variare di i , tutte le permutazioni che hanno una struttura ciclica $[k_1, k_2, \dots, k_n]$ (viene posto $k_j = 0$ se nella partizione non compare j). Si ha così il seguente teorema:

Teorema 3.1.10. *Il numero di classi di coniugio di S_n è uguale al numero delle partizioni di n .*

Esempio 3.5. Determiniamo le classi di coniugio di S_4 . Intanto il suo numero di classi di coniugio è 5 in quanto ci sono 5 partizioni di 4:

$$4 = 1 + 1 + 1 + 1,$$

$$4 = 1 + 1 + 2,$$

$$4 = 1 + 3,$$

$$4 = 2 + 2,$$

$$4 = 4.$$

Si hanno così 5 possibili strutture cicliche: quattro cicli di lunghezza 1, due cicli di lunghezza 1 e uno di lunghezza 2, ecc. Allora si ha:

$$C_1 = \{(1)(2)(3)(4)\} = \{I\},$$

$$C_2 = \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\},$$

$$C_3 = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\},$$

$$C_4 = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

$$C_5 = \{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 3\ 2\ 4)\}.$$

3.2 La classificazione dei gruppi abeliani di ordine p^n , con p primo

Definizione 3.9. Sia p un numero primo qualsiasi, un gruppo finito G viene chiamato p -gruppo quando l'ordine di ogni elemento in G è una potenza di p .

Proposizione 3.2.1. Per ogni p primo, per ogni $n \in \mathbb{N}$, per ogni partizione $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_r]$ di n esiste, a meno di isomorfismi, un solo gruppo abeliano di ordine p^n , denotato con G_λ definito nel seguente modo

$$G_\lambda = \prod_{i=1}^r \mathbb{Z}_{p^{\lambda_i}}.$$

In particolare,

$$|G_\lambda| = p^{\left(\sum_{i=1}^r \lambda_i\right)} = p^n.$$

Da questa proposizione segue subito che:

Date due partizioni diverse, λ e μ , i corrispondenti gruppi, G_λ e G_μ , sono diversi, cioè non sono isomorfi.

Proposizione 3.2.2. Per ogni gruppo abeliano G di ordine p^n esiste una partizione λ di n tale che G è isomorfo a G_λ ($G \cong G_\lambda$).

Quindi i p -gruppi abeliani non isomorfi di ordine p^n sono $p(n)$ qualunque sia il primo p .

In particolare, di ordine p^2 ce ne sono due cioè $\mathbb{Z}_p \times \mathbb{Z}_p$ e \mathbb{Z}_{p^2} ; di ordine p^3 ce ne sono tre cioè $(\mathbb{Z}_p)^3$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ e \mathbb{Z}_{p^3} ; etc

Esempio 3.6. In questo esempio descriviamo tutti i gruppi abeliani di ordine 144.

Il numero 144 lo si può scrivere come

$$144 = 2^4 \cdot 3^2.$$

Il 4 ha le seguenti partizioni:

$$4, 3+1, 2+2, 2+1+1, 1+1+1+1.$$

Di conseguenza si hanno cinque gruppi abeliani non isomorfi di ordine 16: \mathbb{Z}_{16} , $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $(\mathbb{Z}_2)^4$.

Il 2 ha solo due partizioni: 2 e 1 + 1. Si hanno, così, due gruppi abeliani di ordine 9 e cioè \mathbb{Z}_9 e $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Si hanno quindi $5 \cdot 2 = 10$ gruppi abeliani non isomorfi di ordine 144. Essi si possono descrivere anche come segue, usando i risultati noti sul prodotto diretto dei gruppi ciclici \mathbb{Z}_n :

$$\begin{aligned} \mathbb{Z}_{16} \times \mathbb{Z}_9 &= \mathbb{Z}_{144} \\ \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_9 &= \mathbb{Z}_{72} \times \mathbb{Z}_2 \\ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 &= \mathbb{Z}_{36} \times \mathbb{Z}_4 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 &= \mathbb{Z}_{36} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ (\mathbb{Z}_2)^4 \times \mathbb{Z}_9 &= \mathbb{Z}_{18} \times (\mathbb{Z}_2)^3 \\ \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_{48} \times \mathbb{Z}_3 \\ \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_{24} \times \mathbb{Z}_6 \\ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_{12} \times \mathbb{Z}_{12} \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_{12} \times \mathbb{Z}_6 \times \mathbb{Z}_2 \\ (\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \end{aligned}$$

In particolare, questi gruppi abeliani elencati sono scritti in forma canonica: ogni fattore, cioè, ha l'ordine multiplo di quelli che lo seguono e il numero dei fattori è uguale al minimo numero di elementi necessari per generarlo.

Bibliografia

- [1] M. Du Sautoy, *L'enigma dei numeri primi. L'ipotesi di Riemann il più grande mistero della matematica*, ed Bur, 2004;
- [2] S. Mac Lane, G. Birkhoff, *Algebra*, ed Mursia, 1975 - 1985.
- [3] A. Machì, *Gruppi. Una introduzione a idee e metodi della teoria dei numeri*, ed Springer, 2007;
- [4] C. Reid, *Da zero a infinito. Fascino e storia dei numeri.*, ed Dedalo, 1955;
- [5] A. Vistoli, *Note di algebra*, 1993;
- [6] <http://www.ams.org/books/conm/166/conm166-endmatter.pdf>;
- [7] <http://www2.dm.unito.it/paginepersonali/romagnoli/morelli.pdf>;
- [8] <http://matwbn.icm.edu.pl/ksiazki/aa/aa61/aa6131.pdf>;
- [9] <http://www.youtube.com/watch?v=aj4FozCSg8g>;
- [10] <http://www.mi.imati.cnr.it/alberto/mnD23iPART.pdf>;

Ringraziamenti

Il primo ringraziamento desidero rivolgerlo al Professore Libero Verardi per la disponibilità, per i preziosi consigli e per la cura con cui mi ha seguito durante tutta la stesura della tesi.

Grazie a mio padre, a mia madre e a Davide per essermi sempre stati vicino nei momenti più duri e più belli, per avermi ascoltato con pazienza e per essere sempre stati presenti.

Ringrazio i miei coinquilini: Lally, Nico, Ste e Richy per avermi incoraggiato nei momenti più difficili e per avermi aiutato.

Ringrazio le mie amiche matematiche (Samy, Frie, Mary, Livia) con cui ho codiviso la fatica di questi anni di studio e le diverse serate sia bolognesi che riminesi.

Ringrazio, infine, sia le mie più carissime amiche (Chia, Ely e Fedy) che Manuela, Fiore e Giorgia per avermi sostenuto fino ad oggi e per essere stati sempre presenti in ogni momento.