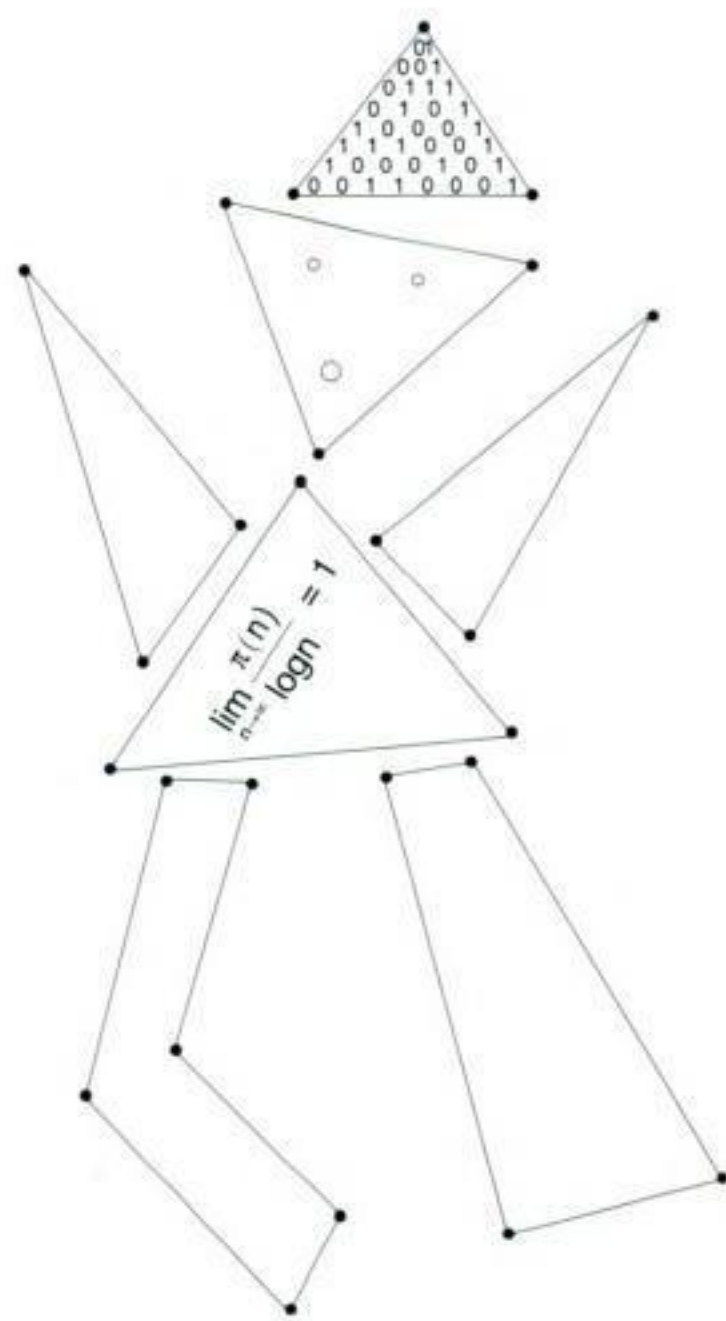


**Luigia Berardi
Albrecht Beutelspacher**

MATEMATICA DISCRETA
Dai fondamenti alle applicazioni



FrancoAngeli

*Collana di matematica
e statistica*

Luigia Berardi, Dipartimento di Ingegneria Elettrica, I-67040 Montelucio di Roio, L'Aquila. Posta elettronica: berardi@ing.univaq.it.

Albrecht Beutelspacher, Mathematisches Institut Justus-Liebig-Universität Arndtstr, 2 D-35392 Giessen. Posta elettronica: albrecht.beutelspacher@math.uni-giessen.de.

Il disegno in copertina è dell'Arch. Diana Eugeni.

1ª edizione. Copyright © 2003 by FrancoAngeli s.r.l., Milano, Italy.

Ristampa

1 2 3 4 5 6 7 8 9

Anno

2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

L'opera, comprese tutte le sue parti, è tutelata dalla legge sui diritti d'autore. Sono vietate e sanzionate la riproduzione con qualsiasi mezzo, formato o supporto comprese le fotocopie (queste ultime sono consentite solo se per uso esclusivamente personale di studio, nel limite del 15% di ciascun volume o fascicolo e alla condizione che vengano pagati i compensi stabiliti), la scansione, la memorizzazione elettronica, la comunicazione e la messa a disposizione al pubblico con qualsiasi mezzo (anche online), la traduzione, l'adattamento totale o parziale.

Stampa: Global Print s.r.l., Via degli Abeti n. 17/1, 20064 Gorgonzola (MI)

I lettori che desiderano informarsi sui libri e le riviste da noi pubblicati possono consultare il nostro sito Internet: www.francoangeli.it e iscriversi nella home page al servizio "Informatemi" per ricevere via e.mail le segnalazioni delle novità o scrivere, inviando il loro indirizzo, a "FrancoAngeli, viale Monza 106, 20127 Milano".

Indice

<u>Introduzione</u>	<u>pag.</u>	<u>7</u>
1. Combinatoria	»	11
1.1. Cardinalità di alcuni insiemi	»	11
<u>1.2. Calcolo combinatorio</u>	»	<u>16</u>
1.3. Principio del cassetto ed applicazioni	»	23
Esercizi	»	25
2. Grafi	»	27
2.1. Concetti fondamentali	»	27
2.2. Grafi connessi e grafi euleriani	»	33
2.3. Grafi di Hamilton	»	38
2.4. Alberi	»	42
2.5. Grafi planari	»	47
2.6. Colorazione dei vertici	»	50
2.7. Colorazione dei lati	»	55
2.8. Grafi bipartiti	»	59
<u>2.9. Algoritmi sui grafi</u>	»	<u>62</u>
Esercizi	»	72
<u>3. Grafi orientati</u>	»	<u>76</u>
<u>3.1. Concetti fondamentali</u>	»	<u>76</u>
<u>3.2. Reti</u>	»	<u>80</u>
3.3. Reti di flusso	»	84
<u>3.4. Le leggi di Kirchhoff</u>	»	<u>89</u>
Esercizi	»	<u>93</u>
<u>4. Numeri</u>	»	<u>97</u>
<u>4.1. Divisione</u>	»	<u>97</u>
<u>4.2. Massimo Comune Divisore</u>	»	<u>100</u>
<u>4.3. Numeri primi</u>	»	<u>104</u>
<u>4.4. Modulo</u>	»	<u>108</u>

4.5. Esistenza dell'inverso di un elemento in Z_n	pag.	110
4.6. Teorema di Eulero	»	111
4.7. Congruenze di primo grado in un'incognita	»	113
Esercizi	»	118
5. Crittologia	»	120
5.1. Fondamenti	»	120
5.2. Cifrari a flusso	»	124
5.3. Cifrari a blocchi	»	130
5.4. Applicazioni	»	134
Esercizi	»	140
6. Crittologia a chiave pubblica	»	144
6.1. Idea della crittologia a chiave pubblica	»	144
6.2. L'algoritmo RSA	»	147
6.3. La forza dell'algoritmo RSA	»	149
6.4. Scambio delle chiavi	»	152
6.5. Schema di Diffie ed Hellman	»	153
6.6. Altri usi del logaritmo discreto	»	155
6.7. Algoritmo del fusto	»	156
6.8. Autenticità della chiave pubblica	»	159
Esercizi	»	161
7. Codici	»	163
7.1. Introduzione	»	163
7.2. Codici rivelatori	»	164
7.3. Nozioni fondamentali	»	169
7.4. Codici correttori	»	170
7.5. Codici lineari	»	173
7.6. Codici di Hamming	»	181
Esercizi	»	186
8. Codici ciclici	»	189
8.1. Codici ciclici	»	189
8.2. Cenni sui campi finiti	»	196
8.3. I codici di Hamming	»	199
8.4. BCH codici 2-correttori	»	200
8.5. Equazioni e loro risoluzione in un campo $GF(2^r)$	»	205
Esercizi	»	210
Bibliografia	»	213
Indici analitico	»	217