

S. Leonesi, C. Toffalori

Numeri e Crittografia

 Springer

Indice

Introduzione	VII
1 Dalla Crittografia ai Numeri	1
1.1 Giulio Cesare e Sherlock Holmes	1
1.2 L'ABC della Crittografia	4
1.3 Esistono Criptosistemi Perfetti?	10
1.4 Crittografia a Chiave Pubblica	17
1.5 Problemi del millennio	19
1.6 Teoria dei Numeri e Crittografia	24
2 Primi e Composti	27
2.1 Divisori, resti e quozienti	27
2.2 Una parentesi computazionale	31
2.3 Il Teorema Fondamentale dell'Aritmetica	33
2.4 Il Teorema dei Numeri Primi	37
2.5 Riconoscere i Primi?	41
2.6 Generare i Primi	42
2.7 Numeri e Misteri	47
3 Potenze, Radici e Logaritmi	51
3.1 Introduzione	51
3.2 L'Aritmetica dell'Orologio	51
3.3 Radici Quadrate e Resti Cinesi	53
3.4 Potenze	57
3.5 Il Piccolo Teorema di Fermat	59
3.6 La funzione ϕ e il Teorema di Eulero	60
3.7 Campi finiti	64
3.8 Logaritmi discreti	68
3.9 I simboli di Legendre e di Jacobi	68
3.10 La Legge di Reciprocità Quadratica di Gauss	76
3.11 Ancora Radici Quadrate	81

3.12	Curve Ellittiche, per finire	82
4	Il Problema della Primalità	91
4.1	Dagli antichi Greci ad <i>AKS</i>	91
4.2	Gli Pseudoprimi di Carmichael	94
4.3	Variazioni sul Piccolo Teorema di Fermat	98
4.4	Primi e <i>NP</i>	101
4.5	L'Algoritmo di Solovay-Strassen	102
4.6	L'Algoritmo di Miller-Rabin	107
4.7	<i>AKS</i> : l'Algoritmo di Agrawal-Kayal-Saxena	114
4.8	Variazioni su <i>AKS</i>	122
5	Il Problema della Fattorizzazione	127
5.1	Introduzione	127
5.2	Il Metodo $p-1$	128
5.3	Il Metodo ρ	129
5.4	Fattorizzazione alla Fermat	132
5.5	Fattorizzazione e Curve Ellittiche	137
5.6	Riflessioni finali	140
6	Ancora Crittografia	143
6.1	Crittografia a Chiave Pubblica	143
6.2	Il Logaritmo Discreto e il Criptosistema di Diffie-Hellman	144
6.3	Doppi Lucchetti	147
6.4	Il Problema dello Zaino	148
6.5	Il Criptosistema <i>RSA</i>	151
6.6	Attacchi a <i>RSA</i>	155
6.7	Crittografia e Curve Ellittiche	157
6.8	Firme digitali	159
6.9	Protocolli a Conoscenza Zero	161
6.10	Testa o Croce telefonico	162
6.11	Poker al telefono	165
	Riferimenti bibliografici	171
	Indice analitico	175