

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

SUMS OF SQUARES OF INTEGERS

CARLOS J. MORENO
SAMUEL S. WAGSTAFF, JR.



Chapman & Hall/CRC
Taylor & Francis Group

Boca Raton London New York

Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Outline of the Rest of the Book	2
1.2.1	Chapter 2	2
1.2.2	Chapter 3	3
1.2.3	Chapter 4	4
1.2.4	Chapter 5	5
1.2.5	Chapter 6	7
1.2.6	Chapter 7	8
1.2.7	Chapter 8	9
2	Elementary Methods	11
2.1	Introduction	11
2.2	Some Lemmas	13
2.3	Two Fundamental Identities	14
2.4	Euler's Recurrence for $\sigma(n)$	18
2.5	More Identities	23
2.6	Sums of Two Squares	26
2.7	Sums of Four Squares	29
2.8	Still More Identities	34
2.9	Sums of Three Squares	38
2.10	An Alternate Method	43
2.11	Sums of Polygonal Numbers	54
2.12	Exercises	57
3	Bernoulli Numbers	61
3.1	Overview	61
3.2	Definition of the Bernoulli Numbers	62
3.3	The Euler-MacLaurin Sum Formula	65
3.4	The Riemann Zeta Function	73
3.4.1	Functional Equation for the Zeta Function	77
3.4.2	Functional Equation for the Dirichlet L -functions	83
3.4.3	Generalized Bernoulli Numbers	89
3.5	Signs of Bernoulli Numbers Alternate	90
3.6	The von Staudt-Clausen Theorem	92

3.7	Congruences of Voronoi and Kummer	95
3.8	Irregular Primes	103
3.9	Fractional Parts of Bernoulli Numbers	107
3.10	Exercises	113
4	Examples of Modular Forms	117
4.1	Introduction	117
4.2	An Example of Jacobi and Smith	118
4.3	An Example of Ramanujan and Mordell	129
4.4	An Example of Wilton: $\tau(n)$ Modulo 23	139
4.4.1	Factorization in Nonnormal Extensions of \mathbb{Q}	145
4.4.2	Table for the Computation of Frobeniuses	147
4.5	An Example of Hamburger	148
4.6	Exercises	153
5	Hecke's Theory of Modular Forms	157
5.1	Introduction	157
5.2	Modular Group Γ and Its Subgroup $\Gamma_0(N)$	158
5.3	Fundamental Domains for Γ and $\Gamma_0(N)$	160
5.4	Integral Modular Forms	161
5.5	Modular Forms of Type $M_k(\Gamma_0(N), \chi)$ and Euler-Poincaré Series	164
5.6	Hecke Operators	166
5.7	Dirichlet Series and Their Functional Equation	168
5.8	The Petersson Inner Product	168
5.9	The Method of Poincaré Series	170
5.10	Fourier Coefficients of Poincaré Series	175
5.11	A Classical Bound for the Ramanujan τ -Function	179
5.12	The Eichler-Selberg Trace Formula	179
5.13	ℓ -Adic Representations and the Ramanujan Conjecture	180
5.14	Exercises	181
6	Representation of Numbers as Sums of Squares	185
6.1	Introduction	185
6.2	The Circle Method and Poincaré Series	186
6.3	Explicit Formulas for the Singular Series	194
6.4	The Singular Series	198
6.4.1	Quadratic Gaussian Sums	198
6.4.2	Ramanujan Sums	205
6.4.3	Fourier Transforms of Gaussian Sums	206
6.4.4	Local Singular Series $L_p(w, \rho_s)$, s Odd and p Odd	211
6.4.5	Local Singular Series $L_2(w, \rho_s)$, s Odd	215
6.4.6	Local Singular Series $L_p(w, \rho_s)$, s Even	219
6.4.7	Examples	222
6.5	Exact Formulas for the Number of Representations	233
6.6	Examples: Quadratic Forms and Sums of Squares	245

6.7	Liouville's Methods and Elliptic Modular Forms	248
6.7.1	The Basic Elliptic Modular Forms	249
6.7.2	Jacobi's Identity: The Origin of Liouville's Methods	253
6.8	Exercises	258
7	Arithmetic Progressions	261
7.1	Introduction	261
7.2	Van der Waerden's Theorem	263
7.3	Roth's Theorem $\tau_3 = 0$	265
7.4	Szemerédi's Proof of Roth's Theorem	271
7.5	Bipartite Graphs	273
7.6	Configurations	279
7.7	More Definitions	291
7.8	The Choice of t_m	295
7.9	Well-Saturated K -tuples	296
7.10	Szemerédi's Theorem	307
7.11	Arithmetic Progressions of Squares	312
7.12	Exercises	315
8	Applications	317
8.1	Factoring Integers	317
8.2	Computing Sums of Two Squares	320
8.3	Computing Sums of Three Squares	325
8.4	Computing Sums of Four Squares	327
8.5	Computing $r_s(n)$	329
8.6	Resonant Cavities	330
8.7	Diamond Cutting	334
8.8	Cryptanalysis of a Signature Scheme	337
8.9	Exercises	340
	References	343
	Index	350