

Presents theories, proofs, and applications

Sums of Squares of Integers

A volume in the *Discrete Mathematics and Its Applications* series

EDITED BY KENNETH H. ROSEN, AT&T LABORATORY, MIDDLETOWN, NEW JERSEY, USA

Carlos J. Moreno

City University of New York Graduate Center and Baruch College, USA

Samuel S. Wagstaff, Jr.

Purdue University, West Lafayette, Indiana, USA

Features

- Contains over 100 exercises to facilitate comprehension
- Presents a proof of Szemerédi's theorem
- Discusses how the modern theory of modular forms complements the classical fundamental results
- Includes applications to fields such as cryptography, crystallography, and thermal radiation

A thorough presentation of number theory

Sums of Squares of Integers covers topics in combinatorial number theory as they relate to counting representations of integers as sums of a certain number of squares. The book introduces a stimulating area of number theory where research continues to proliferate. It is a book of "firsts" – namely it is the first book to combine Liouville's elementary methods with the analytic methods of modular functions to study the representation of integers as sums of squares. It is the first book to tell how to compute the number of representations of an integer n as the sum of s squares of integers for any s and n . It is also the first book to give a proof of Szemerédi's theorem, and is the first number theory book to discuss how the modern theory of modular forms complements and clarifies the classical fundamental results about sums of squares.

The book presents several long-standing, but still interesting and instructive, examples of modular forms. Two chapters develop useful properties of the Bernoulli numbers and illustrate arithmetic progressions, proving the theorems of van der Waerden, Roth, and Szemerédi. The book also explains applications of the theory to three problems that lie outside of number theory in the areas of cryptanalysis, microwave radiation, and diamond cutting. The text is complemented by the inclusion of over one hundred exercises to test the reader's understanding.

Catalog no. C4568, 2006, 368 pp.
ISBN: 1-5848-8456-8, \$89.95 / £39.99

ORDER ONLINE AT [WWW.CRCPRESS.COM](http://www.crcpress.com)

Contents

Introduction

Prerequisites
Outline of Chapters 2 - 8

Elementary Methods

Introduction
Some Lemmas
Two Fundamental Identities
Euler's Recurrence for $\sigma_s(n)$
More Identities
Sums of Two Squares
Sums of Four Squares
Still More Identities
Sums of Three Squares
An Alternate Method
Sums of Polygonal Numbers
Exercises

Bernoulli Numbers

Overview
Definition of the Bernoulli Numbers
The Euler-MacLaurin Sum Formula
The Riemann Zeta Function

See reverse side for continuation of Contents and ordering information



Chapman & Hall/CRC
Taylor & Francis Group

Signs of Bernoulli Numbers Alternate
The von Staudt-Clausen Theorem
Congruences of Voronoi and Kummer
Irregular Primes
Fractional Parts of Bernoulli Numbers
Exercises

Examples of Modular Forms

Introduction
An Example of Jacobi and Smith
An Example of Ramanujan and Mordell
An Example of Wilton: $\tau(n)$ Modulo 23
An Example of Hamburger
Exercises

Hecke's Theory of Modular Forms

Introduction
Modular Group Γ and Its Subgroup $\Gamma_0(N)$
Fundamental Domains For Γ and $\Gamma_0(N)$
Integral Modular Forms
Modular Forms of Type $M_k(\Gamma_0(N), \chi)$ and Euler-Poincaré Series
Hecke Operators
Dirichlet Series and Their Functional Equation
The Petersson Inner Product
The Method of Poincaré Series

Fourier Coefficients of Poincaré Series
A Classical Bound for the Ramanujan τ Function
The Eichler-Selberg Trace Formula
 ℓ -adic Representations and the Ramanujan Conjecture
Exercises

Representation of Numbers as Sums of Squares

Introduction
The Circle Method and Poincaré Series
Explicit Formulas for the Singular Series
The Singular Series
Exact Formulas for the Number of Representations
Examples: Quadratic Forms and Sums of Squares
Liouville's Methods and Elliptic Modular Forms
Exercises

Arithmetic Progressions

Introduction
Van der Waerden's Theorem
Roth's Theorem $\tau_3 = 0$
Szemerédi's Proof of Roth's Theorem
Bipartite Graphs

Configurations
More Definitions
The Choice of t_m
Well-Saturated K -tuples
Szemerédi's Theorem
Arithmetic Progressions of Squares
Exercises

Applications

Factoring Integers
Computing Sums of Two Squares
Computing Sums of Three Squares
Computing Sums of Four Squares
Computing $r_s(n)$
Resonant Cavities
Diamond Cutting
Cryptanalysis of a Signature Scheme
Exercises

References

Index



Please use this ORDER FORM, CALL or ORDER ONLINE at WWW.CRCPRESS.COM

Please indicate quantities next to the title(s) ordered below:

SUMS OF SQUARES OF INTEGERS

.....Catalog no. C4568, ISBN: 1-5848-8456-8 at \$89.95 / £39.99 each.

Other titles of interest:

CRYPTOANALYSIS OF NUMBER THEORETIC CIPHERS

.....Catalog no. C1534, ISBN: 1-58488-153-4, \$82.95 / £41.99

CRYPTOGRAPHY: THEORY AND PRACTICE, THIRD EDITION

.....Catalog no. C5084, ISBN: 1-58488-508-4, \$69.95 / £39.99

AN INTRODUCTION TO CRYPTOGRAPHY

.....Catalog no. C1275, ISBN: 1-5848-8-1275 at \$89.95 / £30.99 each.

Ordering Information: Orders must be prepaid or accompanied by a purchase order. Checks should be made payable to CRC Press. Please add the appropriate shipping and handling charge for each book ordered. All prices are subject to change without notice. If purchasing by credit card please be sure to include the 3 digit security code that appears on the back of your card in the "sec code" field provided below.
U.S./Canada: All orders must be paid in U.S. dollars. TAX: As required by law, please add applicable state and local taxes on all merchandise delivered to CA, CT, FL, KY, MO, NY, and PA. For Canadian orders, please add GST. We will add tax on all credit card orders.
European Orders: All orders must be paid in U.K. £. VAT will be added at the rate applicable.
Textbooks: Special prices for course adopted textbooks may be available for certain titles. To review a book for class adoption, contact our Academic Sales Department or submit your textbook evaluation request online at www.crcpress.com/eval.htm
Satisfaction Guaranteed: If the book supplied does not meet your expectations, it may be returned to us in a saleable condition within 30 days of receipt for a full refund.

SHIPPING AND HANDLING

Region	Delivery Time	First Title	Additional Title	For priority mail services, please contact your nearest CRC PRESS office.
USA/Canada	3-5 Days	\$5.99	\$1.99	
South America	7-14 Days	\$9.99	\$3.99	
Europe	3-5 Days	£2.99	£0.99	
Rest of World	7-21 Days	£4.99	£2.99	

Visa MasterCard American Express Check Enclosed \$

Sec. Code	Exp. Date	Month	Year
-----------	-----------	-------	------

Signature and Telephone Number required on all orders

Signature PO#

Telephone

If you would like to receive information from us by e-mail, please provide your e-mail address below.

E-Mail Address

Name
please print clearly

Company/Institution

Address

City State/Province Zip/Postal Code

Country

ORDERING LOCATIONS

In the Americas:

CRC PRESS

PO Box 409267
Atlanta, GA 30384-9267
Tel: 1-800-272-7737
Fax: 1-800-374-3401

From Outside the Continental U.S.

Tel: 1-561-994-0555
Fax: 1-561-361-6018

e-mail: orders@taylorandfrancis.com

Rest of the World:

CRC PRESS / ITPS

Cheriton House, North Way
Andover, Hants, SP10 5BE, UK
Tel (UK): +44 (0) 1264 34 2926
Tel (Int'l): +44 (0) 1264 34 3070
Fax: +44 (0) 1264 34 3005

e-mail:

(UK): uk.tandf@thomsonpublishingservices.co.uk

(Int'l): international.tandf@thomsonpublishingservices.co.uk

Corporate Offices

CRC PRESS

6000 Broken Sound Parkway, NW, Suite 300
Boca Raton, FL 33487, USA
Tel: 1-800-272-7737
Fax: 1-800-374-3401

From Outside the Continental U.S.

Tel: 1-561-994-0555
Fax: 1-561-361-6018

e-mail: orders@taylorandfrancis.com

CRC PRESS UK

24-25 Blades Court, Deodar Road
London SW15 2NU, UK
Tel: 44 (0) 20 7017 6000
Fax: 44 (0) 20 7017 6747

e-mail: enquiries@crcpress.com