## Advanced Lectures in Mathematics (ALM)

| | |
|---|---|
| ALM 1: | Superstring Theory |
| ALM 2: | Asymptotic Theory in Probability and Statistics with Applications |
| ALM 3: | Computational Conformal Geometry |
| ALM 4: | Variational Principles for Discrete Surfaces |
| ALM 6: | Geometry, Analysis and Topology of Discrete Groups |
| ALM 7: | Handbook of Geometric Analysis, No. 1 |
| ALM 8: | Recent Developments in Algebra and Related Areas |
| ALM 9: | Automorphic Forms and the Langlands Program |
| ALM 10: | Trends in Partial Differential Equations |
| ALM 11: | Recent Advances in Geometric Analysis |
| ALM 12: | Cohomology of Groups and Algebraic K-theory |
| ALM 13: | Handbook of Geometric Analysis, No. 2 |
| ALM 14: | Handbook of Geometric Analysis, No. 3 |
| ALM 15: | An Introduction to Groups and Lattices: Finite Groups and Positive Definite Rational Lattices |
| ALM 16: | Transformation Groups and Moduli Spaces of Curves |
| ALM 17: | Geometry and Analysis, No. 1 |
| ALM 18: | Geometry and Analysis, No. 2 |
| ALM 19: | Arithmetic Geometry and Automorphic Forms |
| ALM 20: | Surveys in Geometric Analysis and Relativity |
| ALM 21: | Advances in Geometric Analysis |
| ALM 22: | Differential Geometry: Under the Influence of S.-S. Chern |
| ALM 23: | Recent Developments in Geometry and Analysis |
| ALM 24: | Handbook of Moduli, Volume I |
| ALM 25: | Handbook of Moduli, Volume II |
| ALM 26: | Handbook of Moduli, Volume III |
| ALM 27: | Number Theory and Related Areas |

Advanced Lectures in Mathematics
Volume XXVII

# Number Theory and Related Areas

edited by

Yi Ouyang · Chaoping Xing · Fei Xu · Pu Zhang

International Press
www.intlpress.com

高等教育出版社
HIGHER EDUCATION PRESS

Advanced Lectures in Mathematics, Volume XXVII
Number Theory and Related Areas

Volume Editors:
Yi Ouyang (University of Science and Technology of China)
Chaoping Xing (Nanyang Technological University, Singapore)
Fei Xu (Capital Normal University, Beijing)
Pu Zhang (Shanghai Jiao Tong University)

Copyright © 2013 by International Press, Somerville, Massachusetts, U.S.A., and by Higher Education Press, Beijing, China.

This work is published and sold in China exclusively by Higher Education Press of China.

All rights reserved. Individual readers of this publication, and non-profit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgement of the source is given. Republication, systematic copying, or mass reproduction of any material in this publication is permitted only under license from International Press. Excluded from these provisions is material in articles to which the author holds the copyright. (If the author holds copyright, notice of this will be given with the article.) In such cases, requests for permission to use or reprint should be addressed directly to the author.

ISBN: 978-1-57146-273-2

Printed in the United States of America.

17 16 15 14 13 1 2 3 4 5 6 7 8 9

ADVANCED LECTURES IN MATHEMATICS

Executive Editors

Shing-Tung Yau
Harvard University

Lizhen Ji
University of Michigan, Ann Arbor

Kefeng Liu
University of California at Los Angeles
Zhejiang University
Hangzhou, China

Editorial Board

Chongqing Cheng
Nanjing University
Nanjing, China

Zhong-Ci Shi
Institute of Computational Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

Zhouping Xin
The Chinese University of Hong Kong
Hong Kong, China

Weiping Zhang
Nankai University
Tianjin, China

Xiping Zhu
Sun Yat-sen University
Guangzhou, China

Tatsien Li
Fudan University
Shanghai, China

Zhiying Wen
Tsinghua University
Beijing, China

Lo Yang
Institute of Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

Xiangyu Zhou
Institute of Mathematics
Chinese Academy of Sciences (CAS)
Beijing, China

*Dedicated to*

*Professor Keqin Feng*

# Contents

**Binary Additive Counter Stream Ciphers**
*Cunsheng Ding, Wenpei Si* .......... **1**

1 Introduction .......... 1
2 Possible attacks and design criteria .......... 3
3 Example 1: the Legendre cipher .......... 9
4 Example 2: the two-prime cipher .......... 14
5 Conclusions and concluding remarks .......... 19
References .......... 21

**Partial Difference Sets from Quadratic Forms and $p$-ary Weakly Regular Bent Functions**
*Tao Feng, Bin Wen, Qing Xiang, Jianxing Yin* .......... **25**

1 Introduction .......... 25
2 Partial difference sets from quadratic forms and uniform cyclotomy .......... 30
3 Partial difference sets from weakly regular $p$-ary bent functions .... 34
References .......... 39

**Governing Fields of the 4-rank of $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{dp})}$ as $p$ Varies**
*Xuejun Guo, Hourong Qin* .......... **41**

1 Introduction .......... 41
2 The governing field of the 4-rank of $K_2\mathcal{O}_F$ .......... 43
3 The governing field of the 8-rank of $K_2\mathcal{O}_F$ .......... 47
References .......... 49

**Word-oriented Linear Feedback Shift Registers: $\sigma$-LFSRs**
*Wenbao Han, Xianghui Liu, Guang Zeng, Gangmin Tan* .......... **51**

1 Introduction .......... 51
2 Model of $\sigma$-LFSR .......... 53
3 Cryptographic properties .......... 55
4 $\sigma$-LFSRs suitable for software implementation .......... 62
5 Application of $\sigma$-LFSRs .......... 65
6 Conclusion .......... 69

References 69

**Statistics of Zeros of Families of $L$-functions over Function Fields: A Survey**
*Wen-Ching Winnie Li, Maosheng Xiong* **73**

1 Introduction 73
2 Hyperelliptic curves 75
3 Cyclic $l$-fold covers of the projective line 78
4 Elliptic curves over a rational function field and generalizations 80
5 Concluding remarks 82
References 82

**Lectures on $p$-adic Zeta Functions and $(\varphi, \Gamma)$-modules**
*Yi Ouyang* **85**

1 Introduction 85
2 Continuous functions, measures and distributions over $\mathbb{Z}_p$ 86
3 The $p$-adic zeta function of Kubota-Leopoldt 111
4 $(\varphi, \Gamma)$-modules and Galois cohomology 118
5 $(\varphi, \Gamma)$-modules and Iwasawa theory 135
References 146

**Conjectures and Results on $x^2$ mod $p^2$ with $4p = x^2 + dy^2$**
*Zhi-Wei Sun* **149**

1 Introduction 149
2 Using Apéry polynomials and products of three binomial coefficients 160
3 Using the polynomials $S_n(x) = \sum_{k=0}^{n} \binom{n}{k}^4 x^k$ 167
4 Using the function $F_n(x) = \sum_{k=0}^{n} \binom{n}{k}^3 \binom{2k}{k} x^{-k}$ 176
5 Using the function $G_n(x) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k} \binom{2n-2k}{n-k} x^{-k}$ 181
6 Using $a_n(x) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} x^k$ 183
7 Miscellaneous things 188
References 195

**Harmonic Weak Maass Forms, Automorphic Green Functions, and Period Integrals**
*Tonghai Yang* **199**

1 Introduction 199
2 Shimura varieties of orthogonal type and their Kudla cycles 203

3 Harmonic weak Maass forms, regularized theta lifting, and automorphic Green functions ........ 205
4 Eisenstein series associated to coherent and incoherent quadratic spaces ........ 210
5 Period integrals of the automorphic Green function $\Phi(z, h; f)$ ........ 213
6 Big CM values of automorphic Green functions ........ 218
References ........ 222

**Some Recent Progress in Higher Koszulity**
*Yu Ye, Pu Zhang* ........ **225**

1 Preliminaries ........ 226
2 Higher Koszulity ........ 227
3 Higher Koszul complexes ........ 228
4 Hilbert and Poincaré series ........ 230
5 Dual algebras and Ext-algebras ........ 232
6 Generalized $d$-Koszul modules ........ 233
7 Lattice distributivity and Koszulity ........ 234
8 More related topics ........ 236
References ........ 238