

<<数论及其相关领域>>

图书基本信息

书名：<<数论及其相关领域>>

13位ISBN编号：9787040367751

10位ISBN编号：7040367750

出版时间：2013-3

出版时间：欧阳毅、等 高等教育出版社 (2013-03出版)

作者：欧阳毅 编

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<数论及其相关领域>>

### 内容概要

《数论及其相关领域(英文)》内容定位于冯克勤教授作出重要成就及感兴趣的领域，分为两个方面：一方面是数论，包括二次丢番图方程的同余性、代数整数环的K群、整体函数域的L-函数、自守形式以及p-adic表示等，另一方面是这些理论在设计、编码等领域的应用，反映了冯克勤教授在数论及其应用领域的发展所作的贡献和影响。

书籍目录

Binary Additive Counter Stream Ciphers 1 Introduction 2 Possible attacks and design criteria 3 Example 1: the Legendre cipher 4 Example 2: the two-prime cipher 5 Conclusions and concluding remarks References Partial Difference Sets from Quadratic Forms and p-ary Weakly Regular Bent Functions 1 Introduction 2 Partial difference sets from quadratic forms and uniform cyclotomy 3 Partial difference sets from weakly regular p-ary bent functions. References Governing Fields of the 4-rank of  $K_{20}^{oa}$  p Varies 1 Introduction 2 The governing field of the 4-rank of  $K_{20}^F$  3 The governing field of the 8-rank of  $K_{20}^F$  References Word-oriented Linear Feedback Shift Registers: a-LFSRs 1 Introduction 2 Model of a-LFSR 3 Cryptographic properties 4 a-LFSRs suitable for software implementation 5 Application of a-LFSRs 6 Conclusion References Statistics of Zeros of Families of L-functions over Function Fields: A Survey 1 Introduction 2 Hyperelliptic curves 3 Cyclic/-fold covers of the projective line 4 Elliptic curves over a rational function field and generalizations 5 Concluding remarks References Lectures on p-adic Zeta Functions and  $(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ -modules 1 Introduction 2 Continuous functions, measures and distributions over  $\mathbb{Z}_p$  3 The p-adic zeta function of Kubota-Leopoldt 4  $(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ -modules and Galois cohomology 5  $(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ -modules and Iwasawa theory References Conjectures and Results on  $x^2 \pmod{p^2}$  with  $4p \mid x^2 + dy^2$  1 Introduction 2 Using Apery polynomials and products of three binomial coefficients 3 Using the polynomials 4 Using the function 5 Using the function 6 Using 7 Miscellaneous things References Harmonic Weak Maass Forms, Automorphic Green Functions, and Period Integrals 1 Introduction 2 Shimura varieties of orthogonal type and their Kudla cycles 3 Harmonic weak Maass forms, regularized theta lifting, and automorphic Green functions 4 Eisenstein series associated to coherent and incoherent quadratic spaces 5 Period integrals of the automorphic Green function  $(z, h; f)$  6 Big CM values of automorphic Green functions References Some Recent Progress in Higher Koszulity 1 Preliminaries 2 Higher Koszulity 3 Higher Koszul complexes 4 Hilbert and Poincare series 5 Dual algebras and Ext-algebras 6 Generalized d-Koszul modules 7 Lattice distributivity and Koszulity 8 More related topics References

## 章节摘录

版权页：插图：6 Conclusion We propose the study of a new family of word-oriented LFSR,s with High Efficiency:  $m$ -LFSRs, which might be interesting in the design of modern stream ciphers. By the theory of matrix and polynomial over finite fields, we explore the cryptographic properties of  $m$ -LFSR.s such as minimal polynomial, state graph, coordinate sequences, and several properties of primitive  $m$ -LFSRs etc. We also discuss some principles for choosing  $m$ -LFSR,s suitable for software implementation, and then we offer an algorithm to search for primitive  $m$ -LFSRs and obtain many primitive  $m$ -LFSR.s such as HHZ-1 or HH2-2, etc, which only use few memory and basic instructions. At last, we give two applications in cryptography: constructing RNGs and stream ciphers. These studies implicate that  $m$ -LFSRs may be used as building block in many cryptographic schemes. We believe that as the performance, security and resource consumption be increasingly important,  $m$ -LFSRs will become an important and attractive alternative to traditional bit and byte oriented designs. However, there remain many open problems for future work. Nevertheless we hope that the results and ideas in this paper serve as an initial step in establishing a continuing research on the design of fast and secure word-oriented LFSRs for cryptographic purpose. Acknowledgement. The work is supported by a grant from the National Natural Science Foundation of China ( No.61003291 ), National Basic Research Program of China ( No.2007CB807902 ), and Foundation for the Author of National Excellent Doctoral Dissertation of China ( No.FANEDD-2007874 ).

## <<数论及其相关领域>>

### 编辑推荐

《数论及其相关领域(英文)》不仅是数论及其应用领域专家们有价值的参考书，也是研究生开展研究时极好的入门书。

<<数论及其相关领域>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>