High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams

Edited by: Alf van der Poorten, *Centre for Number Theory Research, Killara, NSW, Australia*, and Andreas Stein, *University of Illinois at Urbana-Champaign, IL*

A co-publication of the AMS and Fields Institute.

Fields Institute Communications
2004; 392 pp; hardcover
Volume: 41
ISBN-10: 0-8218-3353-7
ISBN-13: 978-0-8218-3353-7
List Price: US$116
Member Price: US$93
Order Code: FIC/41

This volume consists of a selection of papers based on presentations made at the international conference on number theory held in honor of Hugh Williams' sixtieth birthday. The papers address topics in the areas of computational and explicit number theory and its applications. The material is suitable for graduate students and researchers interested in number theory.

Titles in this series are co-published with the Fields Institute for Research in Mathematical Sciences (Toronto, Ontario, Canada).

Readership

Graduate students and research mathematicians interested in number theory.

Table of Contents

of points over a prime field
- S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner -- On a generalization of the radix representation-A survey
- W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski -- Multiplicative structure of values of the Euler function
- W. D. Banks and I. E. Shparlinski -- Congruences and exponential sums with the Euler function
- L. D. Baumert and D. M. Gordon -- On the existence of cyclic difference sets with small parameters
- D. J. Bernstein -- Doubly focused enumeration of locally square polynomial values
- W. Bosma -- Cubic reciprocity and explicit primality tests for $h\cdot 3^k\pm1$
- R. P. Brent and P. Zimmermann -- Algorithms for finding almost irreducible and almost primitive trinomials
- J. Brillhart -- Commentary on Lucas' test
- J. Buchmann, T. Takagi, and U. Vollmer -- Number field cryptography
- D. A. Buell, S. Devarkal, and H. A. Wake -- Reconfigurable computing machines and their applications in computational number theory
- J. Buhler, C. Pomerance, and L. Robertson -- Heuristics for class numbers of prime-power real cyclotomic fields
- H. Cohen -- Counting A_4 and S_4 number fields with given resolvent cubic
- K. Dilcher and J. Knauer -- On a conjecture of Feit and Thompson
- M. García, J. M. Pedersen, and H. te Riele -- Amicable pairs, a survey
- A. Granville -- On the research contributions of Hugh C. Williams
- H. G. Grundman and L. E. Lippincott -- Hilbert modular fourfolds of arithmetic genus one
- E. Herrmann and P. G. Walsh -- Values of ternary recurrence sequences and torsion on certain curves arising from the work of Hugh Williams
- S. Hernández and F. Luca -- Divisibility of exponents of class groups of pure cubic number fields
- J. Holden and P. Moree -- New conjectures and results for small cycles of the discrete logarithm
- M. Jacobson, Jr., A. Menezes, and A. Stein -- Hyperelliptic curves and cryptography
- S. Louboutin -- Remarks on S. Chowla's hypothesis implying that $L(s,\chi)>0$ for $s>0$ and for real characters χ
- S. Müller -- On the computation of cube roots modulo p
- R. D. Patterson and A. J. van der Poorten -- Jeepers, creepers, $\ldots$

- K. Rubin and A. Silverberg -- Algebraic tori in cryptography
- J. P. Sorenson -- An analysis of the generalized binary GCD algorithm
- E. Teske -- An elliptic curve trapdoor system (extended abstract)
- A. J. van der Poorten -- Periodic continued fractions and elliptic curves
- S. S. Wagstaff, Jr. -- The Cunningham project
- A. Weng -- Extensions and improvements for the CM method for genus two
- A. J. van der Poorten and A. Stein -- Advice to referees of submissions to *High Primes and Misdemeanours*