

Number Theory and Applications

edited by

Richard A. Mollin

Department of Mathematics and Statistics,
The University of Calgary, Calgary, Canada



kluwer

the language of science

Table of Contents

PREFACE	xi
PARTICIPANTS	xiii
SCIENTIFIC PROGRAMME	xv
 PART I: Lectures	 1
A. Bremner On the Equation $y^2 = x(x^2 + p)$	3
A. Bremner On the Equation $y^2 = x^3 + k$ Over Function Fields	23
J.W.S. Cassels Arithmetic of Curves of Genus 2	27
J.-M. Deshouillers Waring's Problem and the Circle Method	37
R.K. Guy Tiling the Square With Rational Triangles	45
D.J. Lewis Diophantine Problems: Solved and Unsolved	103
M.E. Pohst Three Principal Tasks of Computational Algebraic Number Theory	123
C. Pomerance Two Methods in Elementary Analytic Number Theory	135
D. Shanks On Gauss and Composition I	163
D. Shanks On Gauss and Composition II	179
N. Stephens Computation of Rational Points on Elliptic Curves Using Heegner Points	205
R. Tijdeman Diophantine Equations and Diophantine Approximations	215
L.C. Washington Number Fields and Elliptic Curves	245
H.G. Zimmer Computational Aspects of the Theory of Elliptic Curves	279

Part II: Contributed Papers	325
J. Buchmann and H. C. Williams On the Existence of a Short Proof For the Value of the Class Number and Regulator of a Real Quadratic Field	327
G. Cornell Group Theory and the Class Group	347
T.W. Cusick A Cantor Set Analog of the Gauss-Kuzmin Theorem	353
J.L. Davison A Class of Transcendental Numbers With Bounded Partial Quotients	365
A.G. Earnest Finiteness Theorems For Number Fields Having Class Groups of Given 2-Power Exponent	373
P. Erdős and J.L. Nicolas On Functions Connected With Prime Divisors of an Integer	381
J.B. Freidlander Shifted Primes Without Large Prime Factors	393
A. Granville On Positive Integers $\leq x$ With Prime Factors $\leq t \log x$	403
A. Granville, J. van de Lune, and H.J.J. te Riele Checking the Goldbach Conjecture on a Vector Computer	423
J.P. Jones Basis for the Kalmar Elementary Functions	435
M. Langevin Systemes Complets de Conjugues sur un Corps Quadratique Imaginaire et Ensembles de Largeur Constante	445
K.S. McCurley Cryptographic Key Distribution and Computation in Class Groups	459
R.A. Mollin and H.C. Williams Class Number One For Real Quadratic Fields, Continued Fractions and Reduced Ideals	481
A.J. van der Poorten Some Facts That Should Be Better Known, Especially About Rational Functions	497
D. Richard Equivalence of Some Questions in Mathematical Logic With Some Conjectures in Number Theory	529
R.J. Stroeker On Diophantine Equations of Type $x^4 - 2ax^2y^2 - by^4 = 1$	547
M.V. Subbarao Addition Chains—Some Results and Problems	555
B.M.M. de Weger A Diophantine Equation of Antoniadis	575

Part III: Problems Session**591**

Unsolved Problems

593

Edited by R.K. Guy

Part IV: Indexes**603**

Name Index

605

Subject Index

611