CONTEMPORARY MATHEMATICS

574

Arithmetic, Geometry, Cryptography and Coding Theory

13th Conference
Arithmetic, Geometry,
Cryptography and Coding Theory
CIRM, Marseille, France
March 14-18, 2011

Geocrypt 2011
Bastia, France
June 19-24, 2011

Yves Aubry
Christophe Ritzenthaler
Alexey Zykin
Editors

American Mathematical Society
Providence, Rhode Island
Contents

Preface vii

Construction of a k-complete addition law on Jacobians of hyperelliptic curves of genus two
CHRISTOPHE ARÈNE and ROMAIN COSSET 1

Number of points in an Artin–Schreier covering
RÉGIS BLACHE 15

Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents
ERIC FÉRARD, ROGER OYONO, and FRANÇOIS RODIER 27

Rational curves with many rational points over a finite field
SATORU FUKASAWA, MASAAKI HOMMA, and SEON JEONG KIM 37

Enumeration of splitting subspaces over finite fields
SUDHIR R. GHORPADE and SAMRITH RAM 49

The characteristic polynomials of abelian varieties of dimension 4 over finite fields
SAFIA HALOUI and VIJAYKUMAR SINGH 59

New bounds on the maximum number of points on genus-4 curves over small finite fields
EVERETT W. HOWE 69

Some planar maps and related function fields
GOHAR M. KYUREGHYAN, FERRUH ÖZBUDAK, and ALEXANDER POTT 87

New families of APN functions in characteristic 3 or 5
ELODIE LEDUCQ 115

Identities for Kloosterman sums and modular curves
PETR LISONEK 125

Degree growth, linear independence and periods of a class of rational dynamical systems
ALINA OSTAFE and IGOR SHPARLINSKI 131

Computer search for curves with many points among abelian covers of genus 2 curves
KARL RÖKAUS 145
CONTENTS

The groups of points on abelian surfaces over finite fields
SERGEY RYBAKOV 151

Computing low-degree isogenies in genus 2 with the Dolgachev–Lehavi method
BENJAMIN SMITH 159

Hodge classes on certain hyperelliptic prymians
YURI G. ZARHIN 171