CAMBRIDGE TRACTS IN MATHEMATICS

General Editors

B. BOLLOBAS, H. HALBERSTAM & C. T. C. WALL

97 Algebraic curves over finite fields

In this Tract, Professor Moreno develops the theory of algebraic curves over finite fields, their zeta and L-functions, and, for the first time, the theory of algebraic geometric Goppa codes on algebraic curves.

Amongst the applications considered are: the problem of counting the number of solutions of equations over finite fields; Bombieri's proof of the Riemann hypothesis for function fields, with consequences for the estimation of exponential sums in one variable; Goppa's theory of error-correcting codes constructed from linear systems on algebraic curves; there is also a new proof of the Tsfasman–Vladut–Zink theorem.

The prerequisites needed to follow this book are few, and it can be used for graduate courses for mathematics students. Electrical engineers who need to understand the modern developments in the theory of error-correcting codes will also benefit from studying this work.

CARLOS MORENO
Professor of Mathematics
Baruch College
City University of New York

Algebraic curves over finite fields

CAMBRIDGE UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1991
First paperback edition 1993

British Library cataloguing in publication data

Moreno, Carlos
Algebraic curves over finite fields.
1. Algebraic curves
I. Title
516.352

Library of Congress cataloguing in publication data available

ISBN 0 521 34252 X hardback
ISBN 0 521 45901 X paperback

Transferred to digital printing 2000

AS

Contents

Preface

This is an introduction to the theory of algebraic curves over finite fields. There are three main themes. The first is a complete presentation of Bombieri's proof of the Riemann hypothesis in the function field case. The second is a full development of the theory of exponential sums in one variable from the point of view of Hasse and Weil. The third and most novel part is the theory of error correcting codes following the program outlined by Goppa. The new results in this last area have come to depend increasingly on many ideas from the theory of modular curves over finite fields and to some extent have motivated our overall presentation. We have included two introductory chapters, one on the basic notions about algebraic curves and the associated function fields, the other including a proof of the Riemann–Roch theorem. In an appendix we verify constructively how the singularities of a plane algebraic curve defined by a homogeneous polynomial in three variables can be transformed into ordinary singularities, i.e. points with distinct tangents, at the expense of increasing the field of constants. This is an essential step in Goppa's program of constructing error correcting codes on algebraic curves from their linear systems. This book fills a gap in the literature of modern number theory; it makes available for the first time all the known results about exponential sums which have applications in algebraic and analytic number theory. Chapter 5 on error correcting codes and the appendix may be studied independently of the rest of the book; they are intended mostly for workers in the field who want to understand the new results about codes on algebraic curves over finite fields.