

Cambridge University Press

978-0-521-45901-3 - Algebraic Curves over Finite Fields

Carlos Moreno

Frontmatter

[More information](#)

CAMBRIDGE TRACTS IN MATHEMATICS

General Editors

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

97 Algebraic curves over finite fields

Cambridge University Press
978-0-521-45901-3 - Algebraic Curves over Finite Fields
Carlos Moreno
Frontmatter
[More information](#)

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.

Cambridge University Press
978-0-521-45901-3 - Algebraic Curves over Finite Fields
Carlos Moreno
Frontmatter
[More information](#)

CARLOS MORENO

*Professor of Mathematics
Baruch College
City University of New York*

*Algebraic curves over
finite fields*



**CAMBRIDGE
UNIVERSITY PRESS**

Cambridge University Press
978-0-521-45901-3 - Algebraic Curves over Finite Fields
Carlos Moreno
Frontmatter
[More information](#)

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

© Cambridge University Press 1991

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

Contents

Preface	ix
1 Algebraic curves and function fields	1
1.1 Geometric aspects	1
1.1.1 Introduction	1
1.1.2 Affine varieties	1
1.1.3 Projective varieties	4
1.1.4 Morphisms	6
1.1.5 Rational maps	8
1.1.6 Non-singular varieties	10
1.1.7 Smooth models of algebraic curves	11
1.2 Algebraic aspects	16
1.2.1 Introduction	16
1.2.2 Points on the projective line \mathbb{P}^1	17
1.2.3 Extensions of valuation rings	18
1.2.4 Points on a smooth curve	20
1.2.5 Independence of valuations	23
Exercises	26
Notes	27
2 The Riemann–Roch theorem	28
2.1 Divisors	28
2.2 The vector space $L(D)$	31
2.3 Principal divisors and the group of divisor classes	32
2.4 The Riemann theorem	36
2.5 Pre-adeles (repartitions)	38
2.6 Pseudo-differentials (the Riemann–Roch theorem)	42
Exercises	46
Notes	47
3 Zeta functions	48
3.1 Introduction	48
3.2 The zeta functions of curves	48
3.3 The functional equation	52
3.3.1 Consequences of the functional equation	57

vi	<i>Contents</i>	
3.4	The Riemann hypothesis	59
3.5	The L -functions of curves and their functional equations	69
3.5.1	Preliminary remarks and notation	69
3.5.2	Algebraic aspects	70
3.5.3	Geometric aspects	76
	Exercises	85
	Notes	87
4	Exponential sums	89
4.1	The zeta function of the projective line	89
4.2	Gauss sums: first example of an L -function for the projective line	91
4.3	Properties of Gauss sums	92
4.3.0	Cyclotomic extensions: basic facts	92
4.3.1	Elementary properties	95
4.3.2	The Hasse–Davenport relation	97
4.3.3	Stickelberger’s theorem	98
4.4	Kloosterman sums	108
4.4.1	Second example of an L -function for the projective line	108
4.4.2	A Hasse–Davenport relation for Kloosterman sums	111
4.5	Third example of an L -function for the projective line	113
4.6	Basic arithmetic theory of exponential sums	114
4.6.1	Part I: L -functions for the projective line	114
4.6.2	Part II: Artin–Schreier coverings	122
4.6.3	The Hurwitz–Zeuthen formula for the covering $\pi: \tilde{\mathcal{C}} \rightarrow \mathcal{C}$	127
	Exercises	131
	Notes	136
5	Goppa codes and modular curves	137
5.1	Elementary Goppa codes	138
5.2	The affine and projective lines	140
5.2.1	Affine line $\mathbb{A}^1(k)$	140
5.2.2	Projective line \mathbb{P}^1	141
5.3	Goppa codes on the projective line	147
5.4	Algebraic curves	153
5.4.1	Separable extensions	154
5.4.2	Closed points and their neighborhoods	155
5.4.3	Differentials	160
5.4.4	Divisors	162
5.4.5	The theorems of Riemann–Roch, of Hurwitz and of the Residue	164
5.4.6	Linear series	170
5.5	Algebraic geometric codes	171
5.5.1	Algebraic Goppa codes	171
5.5.2	Codes with better rates than the Varshamov–Gilbert bound	176

<i>Contents</i>	vii
5.6 The theorem of Tsfasman, Vladut and Zink	178
5.6.1 Modular curves	178
5.6.2 Elliptic curves over \mathbb{C}	179
5.6.3 Elliptic curves over the fields F_p, \mathbb{Q}	184
5.6.4 Torsion points on elliptic curves	188
5.6.5 Igusa's theorem	189
5.6.6 The modular equation	198
5.6.7 The congruence formula	203
5.6.8 The Eichler–Selberg trace formula	208
5.6.9 Proof of the theorem of Tsfasman, Vladut and Zink	210
5.7 Examples of algebraic Goppa codes	211
5.7.1 The Hamming (7, 4) code	212
5.7.2 BCH codes	213
5.7.3 The Fermat cubic (Hermite form)	214
5.7.4 Elliptic codes (according to Driencourt–Michon)	216
5.7.5 The Klein quartic	217
Exercises	220
Appendix Simplification of the singularities of algebraic curves	221
A.1 Homogeneous coordinates in the plane	222
A.2 Basic lemmas	223
A.3 Dual curves	226
A.3.1 Plucker formulas	227
A.4 Quadratic transformations	230
A.4.1 Quadratic transform of a plane curve	231
A.4.2 Quadratic transform of a singularity	233
A.4.3 Singularities off the exceptional lines	234
A.4.4 Reduction of singularities	235
Bibliography	239
Index	245

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.