

CARLOS MORENO

Professor of Mathematics

Baruch College

City University of New York

1

*Algebraic curves over
finite fields*



CAMBRIDGE
UNIVERSITY PRESS

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

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

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 $\mathbb{F}_p, \mathbb{Q}$	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