An Invitation to Arithmetic Geometry

Dino Lorenzini

Graduate Studies in Mathematics
Volume 9

American Mathematical Society

http://dx.doi.org/10.1090/gsm/009

This page intentionally left blank

Other Titles in This Series

9 **Dino Lorenzini,** An invitation to arithmetic geometry, 1996

8 **Winfried Just and Martin Weese,** Discovering modern set theory. I: The basics, 1996

7 **Gerald J. Janusz,** Algebraic number fields, second edition, 1996

6 **Jens Carsten Jantzen,** Lectures on quantum groups, 1996

5 **Rick Miranda,** Algebraic curves and Riemann surfaces, 1995

4 **Russell A. Gordon,** The integrals of Lebesgue, Denjoy, Perron, and Henstock, 1994

3 **William W. Adams and Philippe Loustaunau,** An introduction to Gröbner bases, 1994

2 **Jack Graver, Brigitte Servatius, and Herman Servatius,** Combinatorial rigidity, 1993

1 **Ethan Akin,** The general topology of dynamical systems, 1993

This page intentionally left blank

An Invitation to Arithmetic Geometry

This page intentionally left blank

An Invitation to Arithmetic Geometry

Dino Lorenzini

Graduate Studies
in Mathematics

Volume 9

American Mathematical Society

2000 *Mathematics Subject Classification.* Primary 11-XX, 14-XX;
Secondary 12-XX, 13-XX.

Library of Congress Cataloging-in-Publication Data

Lorenzini, Dino, 1962–
An invitation to arithmetic geometry / Dino Lorenzini.
p. cm. — (Graduate studies in mathematics, ISSN 1065-7339; v. 9)
Includes bibliographical references (p. –) and index.
ISBN 0-8218-0267-4 (hardcover : alk. paper)
1. Arithmetical algebraic geometry. I. Title. II. Series.

QA242.5.L67 1996
512′.74–dc20 95-24459
CIP

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3   17 16 15 14 13 12

To Madeline

A ma mère
Al mio padre

And to those who
fight hunger and poverty

This page intentionally left blank

Contents

Preface

This book grew out of a set of notes from a graduate course in which I tried to introduce the students, in a single course, to both algebraic number theory and the theory of curves. Most books in the literature that touch upon both subjects discuss the function field case from a very algebraic point of view. The modern language of arithmetic geometry is very geometric, and I hope that it will be useful to have in the literature a book such as this with a more geometric introductory presentation of the function field case.

Let us define arithmetic geometry in this preface to be the study of the solutions in k^n of a system of polynomial equations in n variables with coefficients in a ring k (such as $k = \mathbb{Z}$, $k = \mathbb{Q}$, or $k = \mathbb{Z}/p\mathbb{Z}$). While the central problem of arithmetic geometry is thus easily described, mastering the powerful tools developed in the last thirty years to study solutions of polynomials is extremely challenging for beginners[1]. A student with a basic knowledge of algebra and Galois theory will first have to take a course in algebraic number theory, a course in commutative algebra, and a course in algebraic geometry (including scheme theory) to be able to understand the language in which theorems and proofs are stated in modern arithmetic geometry. Moreover, a student who has had the opportunity to take those three courses will be faced with the additional hurdle of understanding their interconnections.

An Invitation to Arithmetic Geometry tries to present in a unified manner, from the beginning, some of the basic tools and concepts in number theory, commutative algebra, and algebraic geometry, and to bring out the deep analogies between these topics. This book introduces the reader to arithmetic geometry by focusing primarily on the dimension one case (that is, curves in algebraic

[1]An example of a polynomial equation in two variables is the Fermat equation $x^n + y^n = 1$. The celebrated Fermat's Last Theorem states that the only solutions in rational numbers to the equation $x^n + y^n = 1$ are the "obvious" ones if $n > 2$. Ribet's proof, in 1986, that Fermat's Last Theorem holds if a weak form of the conjecture of Shimura-Tanyiama-Weil holds is an example of modern tools in arithmetic geometry producing new and deep results about easily stated problems in number theory. Wiles announced on June 23, 1993, that he can prove this weak form of the Shimura-Tanyiama-Weil conjecture and, therefore, that Fermat's Last Theorem holds [**Rib**], [**Fer**].

geometry, rings of dimension one in commutative algebra). Topics covered and interconnected include:

(i) rings of integers, discriminant and ramification, ideal class group (in algebraic number theory),
(ii) localizations, Dedekind domains, discrete valuation rings (in commutative algebra),
(iii) affine and projective curves, the Riemann-Roch theorem (in algebraic geometry), and
(iv) the zeta-function of a curve over a finite field and the analogue of the Riemann hypothesis (in arithmetic geometry).

An example of a fundamental analogy relating these fields of study is the analogy between a ring of integers with its set of archimedian absolute values in number theory, and its analogue in algebraic geometry, an affine curve with its set of points at infinity. This analogy is key to many of the recent translations of statements made in number theory to statements in algebraic geometry, and vice-versa. Unfortunately, this analogy is usually not developed in a course in number theory, nor in a course in algebraic geometry. The present text draws out this and other underlying analogies between these fields.

An Invitation to Arithmetic Geometry is designed as a textbook for a year-long introduction to arithmetic geometry. It includes extensive examples to illustrate each new concept and contains problems at the end of each chapter to help the student grasp the material presented. Most of the results presented in this book are classical and, apart from Bombieri's 1972 proof of the Riemann hypothesis for curves over finite fields, have been in the literature since the 1940s. I have tried to include short historical remarks whenever possible. This book is not designed to be encyclopedic. It introduces new concepts as they are needed and, where possible, uses this need for a concept to motivate its introduction. Our choice to discuss only the case of dimension one means that certain theorems in the text are not stated in their most general form, but only in the form needed for the purposes of the book. When a theorem is not stated in its most general form, references for generalizations of the theorem are included.

While this book is not meant to be an introduction to the theory of schemes, *per se*, I have tried to indicate in the text how the geometric notions introduced relate to schemes (see, e.g., II.7, II.11, VII.**4.17**, and VII.5.**9**). The field of arithmetic geometry has developed tremendously in the last thirty years, and several major open problems have recently been solved, such as Mordell's conjecture XI.1.1 and Fermat's Last Theorem. The proofs of these deep theorems use the language of schemes and the techniques of algebraic geometry. A student of arithmetic geometry needs to master these difficult techniques in addition to the materials presented in this book. I hope that the unified introduction to these topics presented in this book will serve as a motivation for students to learn these techniques and pursue further study of the beautiful interconnections between arithmetic and geometry.

In the course of writing this book, I have received valuable comments on preliminary versions of the manuscript from several colleagues and graduate students. Many thanks to all these people and, in particular, to Ted Chinburg, Hua Chieh Li, Qing Liu, Madeline Morris, Frans Oort, and to Jeff Achter, Glenn Fox, Jon Grantham, Kevin James, Shuguang Li, David Penniston, and Huasong Yin. I have also benefited greatly from the atmosphere of warm collegiality in the University of Georgia Mathematics Department, and especially in its number theory group: William Alford, Sybilla Beckmann, Andrew Granville, Carl Pomerance, and Robert Rumely. Many thanks to my colleagues Brian Boe, Henry Edwards, William Kazez, Ming Jun Lai, and Ted Shifrin for putting up with my questions on software and hardware. Finally, I would like to thank Marilyn Gail Suggs, whose outstanding TeX expertise and typing were invaluable in the preparation of this manuscript.

May 15, 1995 Dino Lorenzini
Athens, Georgia

Glossary of notation

$\alpha \equiv \beta$	congruence modulo an ideal, 3
$\mathcal{O}_L$	ring of integers in a number field L, 13
IJ	product of two ideals, 17
$I + J$	sum of two ideals, 17
$\mathfrak{P}$	prime ideal, 18
$\mathbb{F}_{p^n}$	finite field of order p^n, 19
$\dim A$	dimension of a ring, 28
$Z_f(k)$	zeroes of f with coordinates in k, 35
$\mathbb{A}^1(F), \mathbb{A}^n(F)$	affine line, affine space, 35
$\deg_y(f)$	degree in y of f, 35
$C(Z, F)$	ring of continuous functions from Z to F, 39
π^*	ring homomorphism induced on functions, 39
$\mathbf{x}, \mathbf{y}, \mathbf{g}$	polynomial maps, 40
$\mathrm{Res}(f, g)$	resultant of f and g, 41
$\mathrm{Res}_y(f, g)$	resultant with respect to the variable y, 42
C_f	ring of polynomial functions, 43
$\overline{k}(Z_f)$	field of rational functions, 44
$\mathrm{Max}(A)$	set of maximal ideals of a ring A, 45
p_x, p_y	projections onto the x-axis and y-axis, 48
$\mathrm{Spec}(A)$	spectrum of a ring, 50
$\mathrm{Spec}(\psi)$	map on spectrum induced by a ring homomorphism ψ, 50
$\mathrm{disc}(g)$	discriminant of a polynomial g, 53
$S^{-1}A$	ring of fractions of A with respect to S, 58
$S^{-1}I$	ideal in $S^{-1}A$ generated by the image of an ideal I, 60
A_P	localization of A at P, 61
$S^{-1}M$	module of fractions, 71
$\mathrm{res}_{U,V}$	restriction map, 79
$\{U_i\}_{i \in I}$	open cover, 79
$\mathrm{rank}_A(M)$	rank of an A-module, 81
$V(I)$	closed set in the Zariski topology, 81
$i_P(Z_f(\overline{k}), Z_g(\overline{k}))$	intersection multiplicity at P of $Z_f(\overline{k})$ and $Z_g(\overline{k})$, 83

$P \mid I$	P divides I, 92
$\mathrm{ord}_P(I)$	the order of I at P, 92
$f_{M/P}$	residual degree, 94
$e_{M/P}$	ramification index, 95
$A[\alpha]$	smallest subring of $\overline{K}$ containing A and α, 99
$\mathrm{char}(F)$	characteristic of the field F, 102
$\mu_n(K)$	n-th root of unity in K, 112
$K(\mu_p), K(\zeta_p)$	p-th cyclotomic extension, 112
D_M	decomposition group at M, 117
I_M	inertia group at M, 117
$\mathrm{Frob}(M)$	Frobenius substitution, 120
$(C_f)^G$	ring of invariants, 120
Z/G	quotient space, 121
F_p	Fermat curve, 124
$\mathrm{Norm}_{R/F}$	norm map, 133
$\mathrm{Tr}_{R/F}$	trace map, 134
$\mathrm{N}_{L/K}$	norm map of a field extension, 134
$\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$	discriminant of a basis, 140
$d_{B/A}$	143
$\delta_{B/A}$	143
$\Delta_{B/A}$	discriminant ideal, 145
$N_{B/A}(I)$	ideal-norm of the ideal I, 150
I_A	set of ideals of A, 150
$\mathcal{M}(A)$	monoid of non-zero ideal, 158
$\mathrm{Cl}(A)$	ideal class group, 159
$\\|I\\|_A$	norm of an ideal, 160
h_K	class number of a number field, 164
$\lvert\ \rvert, \lvert\ \rvert_{\mathbb{R}}, \lvert\ \rvert_{\mathbb{C}}$	absolute values, 168
$v, v_p, v_P, v_{\mathfrak{P}}$	valuations, 170
$\lvert\ \rvert_P$	standardized absolute value attached to v_P, 170
$n_{\mathfrak{P}/P}$	171
$V(L)$	set of absolute values of L, 172, 179
$\lvert\ \rvert_\infty, \lvert\ \rvert_\sigma,$	archimedean absolute values, 172
$\mathfrak{R}(s), \mathfrak{J}(s)$	real and imaginary parts, 173
$w \mid \infty$	174
$n_{w/\infty}, n_{w/v}$	174
$\mathcal{O}_v$	local principal ideal domain associated to v, 181
$\mathcal{M}_v$	maximal ideal of $\mathcal{O}_v$, 181
k_v	residue field $\mathcal{O}_v/\mathcal{M}_v$, 182
$\mathcal{V}(L/k)$	set of surjective valuations of L trivial on k, 183
$\mathcal{O}_P$	ring of rational functions defined at P, 184, 214
$\mathcal{O}_X(U)$	ring of functions on U, 184
$\mathbb{P}^n(k)$	points with coordinates in k of the projective n-space, 194
$\mathbb{P}(V)$	projective space, 195

$\mathbb{S}^n$	sphere in $\mathbb{R}^{n+1}$, 196
$(c_0 : \ldots : c_n)$	projective coordinates, 197
$X_F(k)$	set of k-rational points of a plane curve, 199
$f_i(x,y)$	dehomogenization of $F(x_0,x_1,x_2)$, 200
$\varphi_{\mathbb{A}}, \varphi_{\mathbb{P}}$	changes of coordinates, 203
$\rho_{\mathbb{P}(W_m),\mathbb{P}(W_\ell),k}$	projection map, 206
$\rho_{P,L,k}$	projection from a point to a line, 206
$T_{X_F,P}$	tangent line at P to the curve $X_F(\overline{k})$, 208
$k(X_F)$	field of rational functions, 214
$\mathrm{Dom}(\psi)$	domain of a rational function ψ, 214
$\mathcal{O}(U)$	ring of rational functions defined on U, 215
$\overline{C}_f$	227
$\varphi_{(a,b)}, \overline{\varphi}_{(a,b)}$	227
$\psi_{(a,b)}$	228
$k(P)$	field of definition, 230
G_P	stabilizer subgroup of P, 232
$X_{\overline{k}}/\overline{k}$	extension of the scalars, 243
X_F/k	nonsingular complete curve defined by F, 243
φ^*	map on functions associated to a morphism, 245
$\pi_{\overline{k}}$	extension of the scalars, 253
$X(k)$	set of k-rational points, 257
$\deg(P)$	degree of a point, 258
N_n	number of points in $X_F(\mathbb{F}_{q^n})$ or $X(\mathbb{F}_{q^n})$, 259, 269
$\mathrm{Div}(B), \mathrm{Div}(L)$	divisor groups, 260
$\mathrm{div}_B, \mathrm{div}_L$	divisor maps, 260
$\mathrm{Div}(X/k)$	divisor group, 262
div	divisor map, 262
$\mathrm{Pic}(X/k)$	Picard group or divisor class group, 262
cl	class map, 262
deg	degree map on divisors, 264
$\mathrm{Norm}_{X/Y}$	norm map on divisors, 264
$\mathrm{Div}^0(X/k), \mathrm{Pic}^0(X/k)$	kernels of the degree map, 265
$\mathrm{Pic}^d(X/k)$	set of divisor classes of degree d, 266
$\mathrm{Eff}^d(X/k)$	set of effective divisors of degree d, 266
π^*	pull-back map on divisors, 267
$\mathcal{H}_r$	274
$\zeta(s)$	Riemann ζ-function, 274
$\zeta(K,s)$	Dedekind ζ-function, 274
$\zeta(A,s)$	ζ-function of a Dedekind domain, 276
$\mathbf{Z}(X_F/\mathbb{F}_q,T)$	zeta-function, 279, 280, 284
$E_{\mathcal{L}}$	284
g	genus of a curve, 285
w_i	root of $f(T)$, 284
$f(T)$	numerator of the zeta-function of a curve, 285

h	class number of a curve $X/\mathbb{F}_q$, 285
$\mathcal{K}$	canonical class, 289, 319
$J(\rho, \varphi)$	Jacobi sum, 294
$g_a(X)$	Gauss sum, 294
R_K	regulator of a number field, 299
R	regulator in the function field case, 299
$H^0(D)$	306
$h^0(D)$	dimension of $H^0(D)$, 307
$\mathcal{L}(D)_P$	stalk at P of the sheaf $\mathcal{L}(D)$, 310
$H^1(D)$	cohomology group, 311
$h^1(D)$	dimension of $H^1(D)$, 311
$g(X)$	genus of X/k, 311
$\varphi_{E,D}$	map between $H^1(E)$ and $H^1(D)$, 312
$(\alpha)_\infty$	divisor of poles of the function α, 313
$(\alpha)_0$	divisor of zeroes of the function α, 313
$H^\vee$	vector space dual of H, 316
J	vector space of differentials, 317
$\mathrm{Inf}(D, E)$	317
$\mathrm{Sup}(D, E)$	317
$K(j)$	canonical divisor attached to a basis $j \in J$, 319
$\mathrm{Div}_c(K)$	"compactified" divisor group, 321
$\|D\|$	322
M^G	submodules of G-invariants, 324
$p_g, p_g(X_F(D))$	geometric genus, 327
$X_F(\overline{k})^{\mathrm{reg}}$	set of nonsingular points of $X_F(\overline{k})$, 329
$H^0(X_F(\overline{k}), D)$	329
$p_a, p_a(X_F(D))$	arithmetic genus, 331
Frob_R	absolute Frobenius morphism, 339
R^{p^n}	340
α^{1/p^n}	340
$f^{(p^n)}(x, y)$	344
φ^n	n-th Frobenius morphism, 345
F	Frobenius automorphism in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, 349
$\mathrm{Fr}, \overline{\mathrm{Fr}}$	Frobenius endomorphism, 349
$\mathcal{N}_1(X, \sigma)$	358

Index

Bibliography

[AAG] *Arithmetical Algebraic Geometry*, O. Schilling, Editor, Harper & Row, New York, 1965.

[Abh] S. Abhyankar, *Desingularization of plane curves*, Proceedings of Symposia in Pure Mathematics **40** (1983), Part I.

[A-D] D. Anderson and D. Dobbs, Editors, *Zero-dimensional commutative rings*, Marcel Dekker, 1995.

[A-K] A. Altman and S. Kleiman, *Introduction to Grothendieck duality theory*, Lect. Notes in Math. **146**, Springer Verlag, 1970.

[A-M] M. Atiyah and I. McDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass., 1969.

[BDS] *The biographical dictionary of scientists - Mathematicians*, D. Abbot, Editor, Blond Educational, 1985.

[Bom] E. Bombieri, *Counting points on curves over finite fields* (d'après S. A. Stepanov), Séminaire Bourbaki **430** (1972/73).

[Bom2] E. Bombieri, *The Mordell Conjecture Revisited*, Ann. Sc. Norm. Sup. Pisa, Serie IV, **17** (1990), 614-640, and **18** (1991), 473.

[B-K] E. Brieskorn and H. Knörrer, *Plane Algebraic Curves*, Birkhäuser Verlag, Basel, 1986.

[Bou] N. Bourbaki, *Commutative Algebra*, English Edition, Addison-Wesley Publishing Company, 1972.

[C-F] J. Cassels and A. Fröhlich, Editors, *Algebraic Number Theory*, Academic Press, 1967.

[C-S] G. Cornell and J. Silverman, Editors, *Arithmetic Geometry*, Springer-Verlag, New York, 1986.

[Coh] H. Cohn, *Advanced number theory*, Dover Publications, Inc., New York, 1980.

[Cox] D. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, 1989.

[CLO] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[D-K] O. Debarre and M. Klassen, *Points of low degree on smooth plane curves*, J. reine angew. Math. **446** (1994), 81-87.

[D-M] P. Deligne and D. Mumford, *The Irreducibility of the Space of Curves of Given Genus*, Publications IHES **36** (1969), 75-110.

[D-W] R. Dedekind and H. Weber, *Theorie der algebraischen Functionen einer Veränderlichen*, J. reine angew. Math. **92** (1882), 181-290.

[Den] J. Denef, *Report on Igusa's Local Zeta Function*, Séminaire Bourbaki, Astérisque **201-202-203** (1991), 359-386.

[Die] J. Dieudonné, Directeur de la publication, *Abrégé d'histoire des mathématiques* I, Hermann, 1978.

[Die2] J. Dieudonné, *On the History of the Weil Conjectures*, reprinted in E. Freitag and R. Kiehl, Etale Cohomology and the Weil Conjecture, Springer-Verlag, 1988.

[DSB] *Dictionary of Scientific Bibliography*, C. Gillispie, Editor, Charles Schibner's Sons, New York, 1973.

[Edg] H. Edgar, *A number field without an integral basis*, Math. Mag. **52** (1979), 248-251.

[EDM] *Encyclopedic dictionary of mathematics*, English translation of the third edition, K. Itô editor, MIT Press, Cambridge, Massachusetts, 1987.

[Edw] H. Edwards, *Divisor Theory*, Birkhäuser Boston, 1990.

[E-H] D. Eisenbud and J. Harris, *Schemes, the Language of Modern Algebraic Geometry*, Wadsworth & Brooks/Cole, 1992.

[Fal] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. Math. **133** (1991), 549-576.

[Fer] G. Cornell, J. Silverman, and G. Stevens, Editors, *Proceedings of the conference on Fermat's Last Theorem*, held at Boston University in August 1995, Springer Verlag, to appear.

[For] O. Forster, *Lectures on Riemann Surfaces*, Springer-Verlag, 1991.

[Fre] G. Frey, *On the Structure of the Class Group of a Function Field*, Arch. Math. **33** (1979), 33-40.

[Ful] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, W. A. Benjamin, Inc., New York, 1969.

[G-F] V. Gautheron and M. Flexor, *Un exemple de détermination des entiers d'un corps de nombres*, Bull. Sci. Math. **93** (1969), 1-13.

[Gel] S. Gelbart, *An elementary introduction to the Langlands program*, Bull. of the AMS **10** (1984), 177-219.

[Gol] D. Goldfeld, *Gauss' Class Number Problem for Imaginary Quadratic Fields*, Bull. of the AMS **13** (1985), 23-37.

[Gil] R. Gilmer, *Commutative Ring Theory*, in Emmy Noether: a tribute to her life and work, Marcel Dekker, 1981.

[G-R] B. Gross and D. Rohrlich, *Some Results on the Mordell-Weil Group of the Jacobian of the Fermat Curve*, Inv. Math. **44** (1978), 201-224.

[Harb] D. Harbater, in *Number Theory, New York, 1984-85*, Springer LNM **1240**, Springer Verlag (1987), 165-195.

[Harb2] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Inv. Math. **117** (1994), 1-25.

[Har] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[Hil(f)] D. Hilbert, *Théorie des corps de nombres algébriques*, translated by A. Lévy and T. Got, Editions Jacques Gabay, 1991.

[Hil(g)] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, in Gesammelte Abhandlungen, Vol. I, Chelsea Publishing, New York, 1965.

[Hil] H. Hilton, *Plane Algebraic Curves*, Oxford University Press, 1920.

[How] E. Howe, *Constructing distinct curves with isomorphic Jacobians*, J. of Number Theory **26** (1996), 381-390.

[Hut] H. Hutchins, *Examples of commutative rings*, Polygonal Publishing House, 1981.

[I-R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (second edition), Springer-Verlag, New York, 1982.

[Jac] N. Jacobson, *Basic Algebra* I, W. H. Freeman and Company, 1974.

[Ken] K. Kendig, *Elementary Algebraic Geometry*, Springer-Verlag, New York, 1977.

[Kir] F. Kirwan, *Complex algebraic curves*, London Math. Soc. Student Texts **23**, Cambridge Univ. Press, 1992.

[Kna] A. Knapp, *Elliptic Curves*, Princeton University Press, 1992.

[Kob] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer Verlag, 1977.

[Kun] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, translated by Michael Ackerman, Birkhäuser Boston, 1985.

[Lan] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.

[Lan2] S. Lang, *Algebra* (third edition), Addison-Wesley Publishing Company, Inc., 1984.

[Lan3] S. Lang, *Introduction to Arakelov Theory*, Springer-Verlag, New York, 1988.

[Lan4] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[Lan5] S. Lang, *Number Theory III*, Encyclopedia of Mathematical Sciences, vol. 60, Springer-Verlag, 1991.

[Len] H. Lenstra, *Primality Testing*, in Computational Methods in Number Theory, Part I, Mathematical Centre Tracts 154, Mathematisch Centrum, Amsterdam, 1982.

[LMQ] J. Leitzel, M. Madan, and C. Queen, *Algebraic Function Fields with Small Class Number*, J. of Number Theory **7** (1975), 11-27.

[Mac] R. MacRae, *On Unique Factorization in Certain Rings of Algebraic Functions*, J. of Algebra **17** (1971), 243-261.

[M-Q] M. Madan and C. Queen, *Algebraic function fields of class number one*, Acta Arithmetica **XX** (1972), 423-432.

[Mar] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[Mat] H. Matsumura, *Commutative algebra* (second edition), The Benjamin/Cummings Company, Inc., 1980.

[Mat2] H. Matsumura, *Commutative ring theory*, translated by M. Reid, Cambridge University Press, 1986.

[Maz] B. Mazur, *Arithmetic on Curves*, Bull. of the AMS **14** (1986), 207-259.

[Maz2] B. Mazur, *Number Theory as Gadfly*, Am. Math. Monthly **98** (1991), 593-610.

[Mor] C. Moreno, *Algebraic curves over finite fields*, Cambridge University Press, 1991.

[Mum] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties*, Die Grundlehren der math. Wissenschaften, Bd. 221, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

[Mum2] D. Mumford, *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics 1358, Springer Verlag, 1988.

[Mum3] D. Mumford, *Abelian Varieties*, Oxford University Press, 1974.

[Nag] M. Nagata, *Local Rings*, Interscience Publishers, John Wiley & Sons, New York-London-Sydney, 1962.

[Nai] M. Nair, *Power free values of polynomials*, Mathematika **23** (1976), 159-183.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers* (second edition), PWN-Polish Scientific Publishers-Warszawa, 1990.

[Neu] J. Neukirch, *Class Field Theory*, Springer Verlag, 1986.

[Niv] I. Niven, *Formal Power Series*, Am. Monthly **76**, Mathematical Association of America, October 1969, 871-894.

[NTP] *From Number Theory to Physics*, M. Waldschmidt et al. Editors, Springer-Verlag, 1992.

[Per] R. Perlis, *On the Equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. of Number Theory **9** (1977), 342-360.

[Ray] M. Raynaud, *Revêtements de la droite affine en caractéristique* $p > 0$ *et conjecture d'Abhyankar*, Inv. Math. **116** (1994), 425-462.

[Ri] P. Ribenboim, *Algebraic Numbers*, Wiley-Interscience, 1972.

[Ri2] P. Ribenboim, *L'arithmétique des corps*, Hermann, 1972.

[Rib] K. Ribet, *Galois representations and modular forms*, Bull. of the AMS **32** (1995), 375-402.

[Ser1] J.-P. Serre, *Local fields*, Springer Verlag, 1979.

[Ser2] J.-P. Serre, *Algebraic groups and class field*, Springer Verlag, 1988.

[Ser3] J.-P. Serre, *Topics in Galois Theory*, AK Peters, 1992.

[Ser4] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, no. 128 in Oeuvres, Vol. III, Springer Verlag, 1986.

[Ser5] J.-P. Serre, *Facteurs locaux des fonctions zêta*, no. 87 in Oeuvres, Vol. II, Springer Verlag, 1986.

[Ser6] J.-P. Serre, *Motifs*, Journées arithmétiques, 1989, Astérisque **198-200** (1991), 333-349.

[S-T] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492-517, or no. 79 in Serre, Oeuvres, Vol. II, Springer Verlag, 1986.

[SGA] A. Grothendieck, *Séminaire de géometrie algébrique 7, I*, Springer Lecture Notes in Math., **288**, Springer Verlag, 1972.

[Sha] I. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, Berlin and Heidelberg, 1977.

[S-S] H. Shapiro and G. Sparer, *Minimal Bases for Cubic Fields* in Comm. on Pure and Applied Mathematics, Vol. **XLIV** (1991), 1121-1136.

[Sil] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Spr] G. Springer, *Introduction to Riemann surfaces*, Chelsea Publishing Company, New York, 1981.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[Sti2] H. Stichtenoth, *Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. **33** (1979), 357-360.

[Sz] L. Szpiro, *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque **86**, Société Mathématique de France, 1981.

[Szp] L. Szpiro, *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*, Astérisque **127**, Société Mathématique de France, 1985.

[Tat] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer*, In Dix exposés sur la cohomologie des schémas, A. Grothendieck and N. H. Kuiper, Editors, North-Holland (1968).

[Ull] P. Ullrich, *The genesis of Hensel's p-adic numbers*, contributed paper to the "Colloquium Carolus Magnus", Preprint 1995.

[Was] L. Washington, *Introduction to Cyclotomic Fields*, Springer Verlag, 1982.

[Wat] W. Waterhouse, *Introduction to Affine Group Schemes*, Springer Verlag, 1979.

[Wei38b] A. Weil, *Zur algebraischen Theorie der algebraischen Funktionen*, Crelles J. **179**, 129-133, (1938), or in *Oeuvres Scientifiques*, Vol. I, Springer Verlag, 1980.

[Wei39a] A. Weil, *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques*, Revue Scient. 77, pp. 104-106, or in *Oeuvres Scientifiques*, Vol. I, Springer Verlag, 1980.

[Wei40b] A. Weil, *Sur les fonctions algébriques à corps de constantes fini*, C. R. 210, pp. 592-594, or in *Oeuvres Scientifiques*, Vol. I, Springer Verlag, 1980.

[Zak] A. Zaks, *Dedekind k-Subalgebras of* $k(x)$, Comm. in Algebra **5(4)** (1977), 347-364.

[Z-S] O. Zariski and P. Samuel, *Commutative Algebra*, vol. I, Springer Verlag, 1975.

Extremely carefully written, masterfully thought out, and skillfully arranged introduction ... to the arithmetic of algebraic curves, on the one hand, and to the algebro-geometric aspects of number theory, on the other hand. ... an excellent guide for beginners in arithmetic geometry, just as an interesting reference and methodical inspiration for teachers of the subject ... a highly welcome addition to the existing literature.

—Zentralblatt MATH

The interaction between number theory and algebraic geometry has been especially fruitful. In this volume, the author gives a unified presentation of some of the basic tools and concepts in number theory, commutative algebra, and algebraic geometry, and for the first time in a book at this level, brings out the deep analogies between them. The geometric viewpoint is stressed throughout the book. Extensive examples are given to illustrate each new concept, and many interesting exercises are given at the end of each chapter. Most of the important results in the one-dimensional case are proved, including Bombieri's proof of the Riemann Hypothesis for curves over a finite field. While the book is not intended to be an introduction to schemes, the author indicates how many of the geometric notions introduced in the book relate to schemes, which will aid the reader who goes to the next level of this rich subject.

ISBN 978-0-8218-0267-0

9 780821 802670

GSM/9