Translations of
MATHEMATICAL MONOGRAPHS

Volume 170

Elliptic Functions and Elliptic Integrals

Viktor Prasolov
Yuri Solovyev

American Mathematical Society

Selected Titles in This Series

170 **Viktor Prasolov and Yuri Solovyev,** Elliptic functions and elliptic integrals, 1997
169 **S. K. Godunov,** Ordinary differential equations with constant coefficient, 1997
168 **Junjiro Noguchi,** Introduction to complex analysis, 1997
167 **Masaya Yamaguti, Masayoshi Hata, and Jun Kigami,** Mathematics of fractals, 1997
166 **Kenji Ueno,** An introduction to algebraic geometry, 1997
165 **V. V. Ishkhanov, B. B. Lur′e, and D. K. Faddeev,** The embedding problem in Galois theory, 1997
164 **E. I. Gordon,** Nonstandard methods in commutative harmonic analysis, 1997
163 **A. Ya. Dorogovtsev, D. S. Silvestrov, A. V. Skorokhod, and M. I. Yadrenko,** Probability theory: Collection of problems, 1997
162 **M. V. Boldin, G. I. Simonova, and Yu. N. Tyurin,** Sign-based methods in linear statistical models, 1997
161 **Michael Blank,** Discreteness and continuity in problems of chaotic dynamics, 1997
160 **V. G. Osmolovskiĭ,** Linear and nonlinear perturbations of the operator div, 1997
159 **S. Ya. Khavinson,** Best approximation by linear superpositions (approximate nomography), 1997
158 **Hideki Omori,** Infinite-dimensional Lie groups, 1997
157 **V. B. Kolmanovskiĭ and L. E. Shaĭkhet,** Control of systems with aftereffect, 1996
156 **V. N. Shevchenko,** Qualitative topics in integer linear programming, 1997
155 **Yu. Safarov and D. Vassiliev,** The asymptotic distribution of eigenvalues of partial differential operators, 1997
154 **V. V. Prasolov and A. B. Sossinsky,** Knots, links, braids and 3-manifolds. An introduction to the new invariants in low-dimensional topology, 1997
153 **S. Kh. Aranson, G. R. Belitsky, and E. V. Zhuzhoma,** Introduction to the qualitative theory of dynamical systems on surfaces, 1996
152 **R. S. Ismagilov,** Representations of infinite-dimensional groups, 1996
151 **S. Yu. Slavyanov,** Asymptotic solutions of the one-dimensional Schrödinger equation, 1996
150 **B. Ya. Levin,** Lectures on entire functions, 1996
149 **Takashi Sakai,** Riemannian geometry, 1996
148 **Vladimir I. Piterbarg,** Asymptotic methods in the theory of Gaussian processes and fields, 1996
147 **S. G. Gindikin and L. R. Volevich,** Mixed problem for partial differential equations with quasihomogeneous principal part, 1996
146 **L. Ya. Adrianova,** Introduction to linear systems of differential equations, 1995
145 **A. N. Andrianov and V. G. Zhuravlev,** Modular forms and Hecke operators, 1995
144 **O. V. Troshkin,** Nontraditional methods in mathematical hydrodynamics, 1995
143 **V. A. Malyshev and R. A. Minlos,** Linear infinite-particle operators, 1995
142 **N. V. Krylov,** Introduction to the theory of diffusion processes, 1995
141 **A. A. Davydov,** Qualitative theory of control systems, 1994
140 **Aizik I. Volpert, Vitaly A. Volpert, and Vladimir A. Volpert,** Traveling wave solutions of parabolic systems, 1994
139 **I. V. Skrypnik,** Methods for analysis of nonlinear elliptic boundary value problems, 1994
138 **Yu. P. Razmyslov,** Identities of algebras and their representations, 1994
137 **F. I. Karpelevich and A. Ya. Kreinin,** Heavy traffic limits for multiphase queues, 1994
136 **Masayoshi Miyanishi,** Algebraic geometry, 1994
135 **Masaru Takeuchi,** Modern spherical functions, 1994
134 **V. V. Prasolov,** Problems and theorems in linear algebra, 1994
133 **P. I. Naumkin and I. A. Shishmarev,** Nonlinear nonlocal equations in the theory of waves, 1994
132 **Hajime Urakawa,** Calculus of variations and harmonic maps, 1993

(*Continued in the back of this publication*)

This page intentionally left blank

Elliptic Functions and Elliptic Integrals

This page intentionally left blank

10.1090/mmono/170

Translations of

MATHEMATICAL MONOGRAPHS

Volume 170

Elliptic Functions and Elliptic Integrals

Viktor Prasolov
Yuri Solovyev

American Mathematical Society
Providence, Rhode Island

В. В. Прасолов
Ю. П. Соловьёв

ЭЛЛИПТИЧЕСКИЕ ФУНКЦИИ И ЭЛЛИПТИЧЕСКИЕ ИНТЕГРАЛЫ

Translated from the original Russian manuscript by D. Leites

1991 *Mathematics Subject Classification.* Primary 11-01, 14H52, 33E05.

ABSTRACT. This book is devoted to geometry and arithmetic of elliptic curves and to elliptic functions with applications to algebra and number theory. It includes modern interpretations of some famous classical algebraic theorems such as Abel's theorem on lemniscate and Hermite's solution of the fifth degree equation by means of theta functions. The book is self-contained and assumes as prerequisites only the standard one-year courses in algebra and analysis.

Library of Congress Cataloging-in-Publication Data

Prasolov, V. V. (Viktor Vasil′evich)
Elliptic functions and elliptic integrals / Viktor Prasolov, Yuri Solovyev.
p. cm. — (Translations of mathematical monographs, ISSN 0065-9282 ; v. 170)
"Translated from the original Russian manuscript by C. Leites"—T.p. verso.
Includes bibliographical references and index.
ISBN 0-8218-0587-8
1. Elliptic functions. I. Solov′ev, I͡U. P. (I͡Uriĭ Pavlovich) II. Title. III. Title: Ėllipticheskie funkt͡sii i ėllipticheskie integraly IV. Series.
QA343.P73 1997
515′.983—dc21 97-24309
CIP

---

10 9 8 7 6 5 4 3 2 1 02 01 00 99 98 97

Contents

Preface ix

Chapter 1. Geometry of Cubic Curves 1
§1.1. Addition of points on a cubic 1
§1.2. Lines and curves on the projective plane 8
§1.3. The tangents and inflection points 11
§1.4. Normal forms of the nonsingular cubic 16
§1.5. Singular cubics 20
§1.6. No nonsingular cubic admits a rational parameterization 22

Chapter 2. Elliptic Functions 25
§2.1. The topological structure of nonsingular cubics in $\mathbb{C}P^2$ 26
§2.2. The elliptic functions 29
§2.3. The Weierstrass function 32
§2.4. A differential equation for the Weierstrass function $\wp(z)$ 35
§2.5. A parameterization of the cubic with the help of the Weierstrass function 36
§2.6. The elliptic integrals 39
§2.7. Addition theorems for the elliptic integrals $F(\varphi)$ and $E(\varphi)$ 44
§2.8. The elliptic Jacobi functions 46
§2.9. The Weierstrass theorem on functions possessing an algebraic addition theorem 49

Chapter 3. Arcs of Curves and Elliptic Integrals 53
§3.1. Arcs of the ellipse and the hyperbola 53
§3.2. Division of arcs of the ellipse 55
§3.3. Curves with elliptic arcs 60
§3.4. Curves whose arc lengths can be expressed in terms of arc lengths of the circle 64

Chapter 4. Abel's Theorem on Division of Lemniscate 67
§4.1. Construction of a regular 17-gon. An elementary approach 69
§4.2. Construction of regular polygons. Elements of Galois theory 71
§4.3. The equation for the division of the lemniscate 78
§4.4. Proof of Abel's theorem on the division of the lemniscate 86
§4.5. Several remarks on Serret's curves 91

Chapter 5. Arithmetic of Cubic Curves 103
§5.1. Diophantus' method of secants. Second degree diophantine equations 104

§5.2. Addition of points on a cubic curve 111
§5.3. Several examples 115
§5.4. Mordell's theorem 119
§5.5. The rank and the torsion group of an elliptic curve 124

Chapter 6. Algebraic Equations 131
§6.1. Solving cubic and quartic equations 131
§6.2. Symmetric polynomials 133
§6.3. The Lagrange resolvents 134
§6.4. Roots of unity 137
§6.5. The Abel theorem on the unsolvability in radicals of the general quintic equation 140
§6.6. The Tschirnhaus transformations. Quintic equations in Bring's form 145

Chapter 7. Theta Functions and Solutions of Quintic Equations 149
§7.1. Definition of theta functions 149
§7.2. Zeros of theta functions 150
§7.3. The relation $\Theta_3^4 = \Theta_2^4 + \Theta_0^4$ 151
§7.4. Representation of theta functions by infinite products 152
§7.5. The relation $\Theta_1'(0) = \pi\Theta_0(0)\Theta_2(0)\Theta_3(0)$ 154
§7.6. Dedekind's η-function and the functions f, f_1, f_2 155
§7.7. Transformations of theta functions induced by transformations of τ 156
§7.8. The general scheme of solution of quintic equations 158
§7.9. Transformations of order 5 159
§7.10. The change of parameter $\tau \mapsto \tau + 2$ 160
§7.11. The change of parameter $\tau \mapsto -\frac{1}{\tau}$ 161
§7.12. The change of parameter $\tau \mapsto \frac{\tau-1}{\tau+1}$ 163
§7.13. Functions invariant with respect to the changes of parameter $\tau \mapsto \tau + 2$, $\tau \mapsto -\frac{1}{\tau}$ and $\tau \mapsto \frac{\tau-1}{\tau+1}$ 164
§7.14. Deduction of the modular equation 165
§7.15. Solving quintic equations 166
§7.16. The main modular function $j(\tau)$ 169
§7.17. The fundamental domain of $j(\tau)$ 170
§7.18. How to solve the equation $j(\tau) = c$ 173
§7.19. The functions invariant under the changes of parameter $\tau \mapsto \tau + 1$ and $\tau \mapsto -\frac{1}{\tau}$ 175
§7.20. The functions invariant with respect to the changes of parameter $\tau \mapsto \tau + 2$ and $\tau \mapsto -\frac{1}{\tau}$ 176

Bibliography 179

Index 183

Preface

In June of 1796 the Literature Gazette, published at that time in Jena, offered to its readers the following note (in German):

New Discoveries.

Every novice in geometry knows that it is possible to construct geometrically, i.e., by ruler and compass, various regular polygons, namely, a triangle, a pentagon, a 15-gon and the polygons one can obtain from each of these by consecutive doubling the number of its sides. This was known already in the time of Euclid and, it seems, that the reigning belief, starting from that time, is that the domain of elementary geometry does not surpass these limits: at least I do not know any successful attempt to expand it in this direction. Hence, the discovery that, apart from these regular polygons, it is possible to geometrically construct a multitude of other polygons, for example, a 17-gon, seems to me worth noting. This discovery is essentially a mere corollary of a far-reaching theory not completely finished yet. The moment this theory is completed it will be offered to the public.

C. F. Gauss from Braunschweig,
student of mathematics in Göttingen.

The theory was completed five years later and published by Gauss in the 7th section of the famous *Disquisitiones Arithmeticae* (*Arithmetical Studies*), which appeared in 1801. Gauss proved that if the number n of sides of a regular polygon is of the form $n = 2^a p_1 \cdots p_k$, where the p_i are distinct Fermat primes, i.e., prime numbers of the form $2^{2^m} + 1$, then the polygon can be constructed by ruler and compass. In algebraic language this statement means that for the numbers n indicated the equation $x^n - 1 = 0$ is solvable in quadratic radicals.

The proof of Gauss' theorem is based on a neat algebraic theory which served as the cornerstone for Galois theory created thirty years after *Arithmetical Studies* was published.

In the 7th section of *Arithmetical Studies*, apart from the theory of division of the circle, i.e., the algebraic theory of circular functions, there is a short remark, also by Gauss, to the effect that the method he developed is also applicable to certain higher transcendental functions; in particular, to functions related with integrals of the form $\int \frac{dx}{\sqrt{1-x^4}}$.

This remark became a starting point for the studies of Abel, who in 1827 proved that for the same values of n as mentioned by Gauss, it is possible to divide Bernoulli's lemniscate by ruler and compass into n equal parts. To do that, Abel had to considerably improve Gauss' method and, what is most important, create a new mathematical discipline — the *theory of elliptic functions*.

The theory of elliptic functions and its geometric twin — the *theory of elliptic curves* — occupies one of the central places in mathematics having unified several of its branches. In spite of its senior age, the theory of elliptic functions and elliptic curves remains an alive and rapidly developing domain of mathematics; it is an inexhaustible source of techniques, problems, and conjectures for the researchers.

In the past decade elliptic functions and curves became the subject of close attention by experts in such nonclassical fields as algebraic topology and quantum field theory; quite recently with the help of the elliptic curve theory Fermat's Last Theorem was finally proved.

The main topics of this book are the geometry of cubic curves, elliptic functions and their properties, elliptic integrals, addition theorems for elliptic functions and integrals, arcs of algebraic curves expressible via elliptic integrals, Abel's theorem on lemniscate, arithmetic properties of elliptic curves, Mordell's theorem, theta functions, and solutions of equations of the fifth degree.

In other words, the book is an introductory course on the theory of elliptic functions and elliptic curves and is aimed at those who encounter this topic for the first time. However, we hope that the book will be of interest to the experts as well.

The book is based on three lectures written by one of us (Yu. S.) in 1991–1992 as part of lectures for students organized by the Moscow Mathematical Society. The material of the book was collected for the optional course given by the second author (V. P.) in 1992–1993 at the Independent University of Moscow.

In writing this book we used a vast selection of literature, both classical treatises and various modern papers. We were greatly influenced by a remarkable paper by M. Rosen from *American Mathematical Monthly* [**C14**] that contains a modern proof of Abel's theorem. We have also borrowed a lot of useful facts from wonderful books of Husemoller [**B10**], Koblitz [**B12**] and Stepanov [**B22**].

The book does not assume from the reader any knowledge beyond the limits of beginning courses of mathematics majors in universities and is oriented to the widest range of readers: students of mathematics and physics, teachers, and even high school students. We hope that, having been acquainted with the subject of this book, the reader will be able to feel the charm of the fine art that we experienced while deciphering the works of old masters.

While the book was being written V. Prasolov benefited from a grant from the Russian Fund for Basic Research (95-01-00846).

Bibliography

A. Classical works

[A1] N. H. Abel, *Oeuvres complètes du Niels Henrik Abel*, Christiania, 1881.

[A2] J. Bernoulli, *Opera Omnia, T. I–IV*, Bosquet, Lausanne, Genevae, 1742.

[A3] Diophantus of Alexandria, *Arithmetics and Book on Polygonal Numbers*, Translated from the ancient Greek by I.N. Veselovsky, ed. and commented by I.G. Bashmakova, Nauka, Moscow, 1974 (in Russian); see also id. edited by Paulus Tannery, *Opera Omnia cum Graecis Commentariis*, Teubner, 2 vols., 1893–1895.

[A4] L. Euler, *Opera Omnia, Ser. I. T. XXI, 91–118*, Leipzig, 1911–1956.

[A5] ______, *Introduction to analysis of the infinitesimals, Book 9, ch. VI.*, Bosquet, Cop., 1988.

[A6] G. Fagnano, *Produzioni mathematiche. Opere Mathematiche del Marchese Giulio Carlo de' Toschi di Fagnano*, see also id., 3 vols., 1911–1913, 1750.

[A7] C. F. Gauss, *Arithmetische Untersuchungen*, Chelsea, New York, 1965.

[A8] ______, *Werke, Bd. 10.*, Göttingen, 1917.

[A9] Ch. Hermite, *Oeuvres,* tome 2, (1) Sur la résolution de l'equation du cinquième degrée, pp. 5–12; (2) Sur l'equation du cinquième degrée, pp. 347–424, Gauthier-Villars, Paris, 1908.

[A10] C. G. J. Jacobi, *Gesammelte Werke*, Band I–VII, Berlin, 1881–1891; Chelsea, New York, ???.

[A11] J. L. Lagrange, Mém. Acad. Berlin (1770–1771).

[A12] A. M. Legendre, *Traite des fonctions elliptiques et des integrales Euleriennes,* t.1–3, Paris, 1825–1832.

[A13] H. Poincaré, *Sur les propriétés des courbes algebriques planes*, J. Liouville **7** (1901), 161–233.

[A14] Serret J.-A., *Cours de calcul différentiel et intégral,* t. 1–3, 2-éme publ., Gauthier-Villars, Paris, 1879.

[A15] E. W. von Tschirnhaus, *Nova Metodus Auferendi Omnes Terminos Intermedios ex Data Aequatione*, Acta eruditorum, Bd. 2, Leipzig, 1683.

B. Main textbooks

[B1] N. I. Akhiezer, *Elements of the theory of elliptic functions*, Amer. Math. Soc., Providence, RI, 1990.

[B2] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.

[B3] N. Bourbaki, *Algèbre,* Ch. 4–17, Masson, Paris, 1981.

[B4] E. Brieskorn and H. Knörrer, *Plane algebraic curves*, Birkhäuser, Basel, 1986.

[B5] W. S. Burnside and A. W. Panton, *The theory of equations*, Dublin Univ. Press, Dublin–London, 1928.

[B6] H. M. Edwards, *Galois theory*, Springer-Verlag, Heidelberg, 1984.

[B7] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Bd.1, 1916; Bd.2, 1922, Teubner, Leipzig-Berlin.

[B8] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Wiley, 1978.

[B9] A. Hurwitz, *Vorlesungen über allgemeine Funktionentheorie und elliptische Functionen*, Vierte Auflage, Springer-Verlag, Heidelberg, 1964.

[B10] D. Husemoller, *Elliptic curves*, Springer-Verlag, Heidelberg, 1987.

[B11] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd edition, Springer-Verlag, Heidelberg, 1990.

[B12] M. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, Heidelberg, 1984.

[B13] M. Kline, *Mathematical thought from ancient to modern times*, Oxford University Press, New York, 1972.

[B14] S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, Heidelberg, 1983.

[B15] ———, *Elliptic functions*, 2nd edition, Springer-Verlag, Heidelberg, 1987.

[B16] A. I. Markushevich, *The theory of functions of a complex variable*, 3 vols., 1965–1967, Prentice Hall, Englewood Cliffs, NJ.

[B17] L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.

[B18] E. J. F. Primrose, *Plane algebraic curves*, Macmillan, London, 1955.

[B19] A. Robert, *Elliptic curves*, Lecture Notes in Math., vol. 326, Springer-Verlag, Heidelberg, 1973.

[B20] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Heidelberg, 1986.

[B21] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, Heidelberg, 1994.

[B22] S. A. Stepanov, *The arithmetic of algebraic curves*, "Nauka", Moscow, 1991. (Russian)

[B23] R. J. Walker, *Algebraic curves*, Dover, New York, 1950.

[B24] H. Weber, *Lehrebuch der Algebra, Bd. 3. Elliptische Funktionen und algebraische Zahlen*, Braunschweig, 1908.

[B25] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Springer-Verlag, Heidelberg, 1976.

[B26] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, 4th edition, vol. 1–2, Cambridge Univ. Press, Cambridge, 1927.

C. Selected articles

[C1] B. J. Birch, *Conjectures on elliptic curves*, Theory of Numbers, Proc. Symp. Pure Math., vol. 8, Amer. Math. Soc., Providence, RI, 1963.

[C2] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves,* I, II, J. Reine und Angew. Math. **212** (1963), 7–25; **218** (1965), 79–108.

[C3] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[C4] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[C5] F. J. Grunewald and R. Zimmert, *Über einige rationale elliptische Kurven mit freiem Rang* > 8, J. Reine Angew. Math. **296** (1977), 100–107.

[C6] H. Hasse, *Abstrakte Begrundung der komplexen Multiplication und Riemannsche Vermutung in Funktionenkorpern*, Abh. Math. Sem. Hamburg **10** (1934), 325–348.

[C7] L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math. **11** (1950), 238–244.

[C8] J. Igusa, *On the transformation theory of elliptic functions*, Amer. J. Math. **81** (1959), 436–452.

[C9] B. Mazur, *Rational points on modular curves*, Lecture Notes in Math., vol. 601, Springer-Verlag, Heidelberg, 1976.

[C10] I. G. Melnikov, *The problem of division of the lemniscate,* I, II, Uchenye Zapiski Leningrad. Gos. Pedagogicheskogo Inst. **197** (1958), 20–38; 39–42. (Russian)

[C11] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[C12] ———, *The infinity of rational solutions of* $y^2 = x^3 + k$, J. London Math. Soc. **41** (1966), 523–525.

[C13] ———, *On the magnitude of the integral solutions of the equation* $ax^2+by^2+cz^2 = 0$, J. Number Theory **1** (1969), 1–3.

[C14] M. Rosen, *Abel's theorem on the lemniscate*, Amer. Math. Monthly **88** (1981), 387–395.

[C15] T. Soundararajan, *On the automorphisms of the complex number field*, Math. Mag. **40** (1967), 213.

[C16] J. Tate, *The arithmetics of elliptic curves*, Invent. Math. **23** (1974), 179–206.
[C17] A. Weil, *Sur une théorème de Mordell*, Bull. Sci. Math. (2) **54** (1930), 182–191.
[C18] P. B. Yale, *Automorphisms of the complex numbers*, Math. Mag. **39** (1966), 135–141.
[C19] D. Zagier, *A one-sentence proof that every prime* $p = 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), 144.

This page intentionally left blank

Index

C_n, 71
$E(\varphi)$, 43
$E(\mathbb{Q})$, the set of rational points on the curve E, 115
$F(\varphi)$, 43
K_n, 72
L-function of a rational elliptic curve, 126
S_p, Serret's curve, 95
$\text{Tors}\, E(\mathbb{Q})$, 124
$\text{cn}\, u$, 47
$\text{dn}\, u$, 47
$\equiv$ as identically equal to, 5
η-function, Dedekind's, 160
$\eta(\tau)$, Dedekind's η-function, 160
$\widehat{BM}$, the length of $\smile BM$, 55
$\text{sn}\, u$, 47
$\text{am}\, u$, the amplitude, 47
$\wp(z)$, the Weierstrass function, 32
$f(\tau)$, 155
$f_1(\tau)$, 155
$f_2(\tau)$, 155
j-invariant, 101
$j(\tau)$, 169
r_E, 124

Abel, 26, 68, 140
Abel's theorem, 140
algebraic addition theorem, 49
amplitude, 47
automorphisms, trivial, 101
axes, principal, 58

basis of transcendentality, 78
Bernoulli, 68
Bernoulli's lemniscate, 25, 68
Bernoulli, Nicholas, 40
Birch, 125
blow-up, 93
Bring, 147

Cassini, 67
Cassini's ovals, 68
chain, 76
complex multiplication, 101
conic, 1
conjugate (diameters), 58
cubic, 1, 131
cubic, nonsingular, 16
curve, algebraic, 1
curve, elliptic associated with Serret's curve, 97
curve, Serret, 95

Dedekind function, 160
Descartes, 103
diagram, Newton, 99
diameters, conjugate, 58
diophantine equation, 103
Diophantus, 103
division of arcs, 55
division of the arc "by half", 56
domain, fundamental, 173
doubly periodic function, 29
duality, projective, 18
duplication of the arc, 56

Eisenstein, 68, 84
Eisenstein's theorem, 85
element, primitive, 139
ellipse, 25
elliptic integral, 43, 54
elliptic Jacobi functions, 46, 47
equation, cubic, 131
equation, general, 140
equation, modular, 166
equation, quartic, 131
equation, resolving, 136
equation, solvable in radicals, 140
Euclid, 103
Euler, 25, 64, 68
Euler formula, 12
exponential, 50

Fagnano, 25, 60, 68
Fagnano's theorem, 56
Fermat, 104, 118
Fermat primes, 68
field, normal or Galois, 140
form, Legendre, 42
form, Weierstrass, 16, 42
formula, Euler, 12
Fueter, 118
function, doubly periodic, 29

function, elliptic, 29
function, elliptic Jacobi, 31, 47
function, meromorphic, 29
function, Weierstrass, 31, 32
fundamental domain, 173
fundamental parallelogram, 29

Galois field, 140
Gauss, 26, 68
generic lines, 18
generic points, 18
genus of the curve, 98
group of substitutions, 140
group, torsion of the elliptic curve, 124

Hasse, H., 126
Hermite, 131
Hesse curve, 13
Hessian, 13
Holzer, 109

inflection point, 13
integral, elliptic, 43, 54
involution, 89

Jacobi, 26
Jacobi elliptic function, 31

Lagrange's resolvent, 135
Legendre, 26, 60, 107
Legendre form, 42
Legendre's theorem, 41
Leibniz, 40, 145
lemniscate, 67
lemniscate, Bernoulli, 25, 68
lexicographically ordered monomials, 133
lines, generic, 18

Möbius transformation, 159
Main theorem on symmetric polynomials, 133
Mazur, 128
Mazur's theorem, 128
meromorphic function, 29
Mesiriac, 104, 118
Mestre, 125
method of secants, 104
modular equation, 166
Mordell, 118, 119
Mordell's theorem, 119
multiplicity, 93

Newton diagram, 99
normal field, 140
normal form, Weierstrass', 16
normal forms of a nonsingular cubic, 16
number, congruent, 111
numbers, complex, odd, 81

odd complex numbers, 81
order of a point, 114
order of the elliptic function, 31
ovals, Cassini, 68

Pappus's theorem, 5
parallelogram, fundamental, 29
Pascal's theorem, 1, 4
Picard's big theorem, 51
Plücker, J., 7
Poincaré, A., 119
point, fixed, 89
point, inflection, 13
point, nonsingular of the curve, 12
point, simple, 93
point, singular, 93
point, the order of, 114
points, generic, 18
primitive element, 139
primitive root, 137
principal axes, 58
projective duality, 18
projective plane, 9

quartic, 131

rank of the elliptic curve, 124
rationality field, 140
reduction of the curve modulo p, 125
Regiomontanus, 103
resolvents, Lagrange's, 135
resolving equation, 136
resultant, 14
Rosen, 68, 86
Ruffini, Paulo, 140

Serret, 64
Serret's curve, 95
Serret's theorem, 62
Serret, Joseph-Alfred, 61
set, Zorn closed, 76
solution, integer, 103
solution, rational, 103
Steiner, J., 7
sum of points, 1
Swinnerton–Dyer, 125
symmetric, 133
symmetric polynomials, elementary, 133

tangent to the curve, 12
theorem, Abel, 140
theorem, algebraic addition, 49
theorem, Eisenstein, 85
theorem, Fagnano, 56
theorem, Legendre, 41
theorem, Mazur, 128
theorem, Mordell, 119
theorem, on symmetric polynomials, main, 133
theorem, Pappus, 5
theorem, Pascal, 1, 4
theorem, Picard's big, 51
theorem, Serret, 62

theorem, Viéta, 166
theorem, Weierstrass, 50
theta constants, 151
theta functions, 150
trace, 123
transcendentality, basis of, 78
transformation, fractional linear, 159
transformation, Möbius, 159
transformation, Tschirnhaus, 146
Tschirnhaus, E.W. von, 145
Tschirnhaus's transformation, 146

Viéta theorem, 166

Weber, 131
Weierstrass form, 16, 42
Weierstrass function, 31, 32
Weierstrass' theorem, 50
Wiles, A., 126

Zagier, 89

Selected Titles in This Series

(Continued from the front of this publication)

131 **V. V. Sharko,** Functions on manifolds: Algebraic and topological aspects, 1993
130 **V. V. Vershinin,** Cobordisms and spectral sequences, 1993
129 **Mitsuo Morimoto,** An introduction to Sato's hyperfunctions, 1993
128 **V. P. Orevkov,** Complexity of proofs and their transformations in axiomatic theories, 1993
127 **F. L. Zak,** Tangents and secants of algebraic varieties, 1993
126 **M. L. Agranovskiĭ,** Invariant function spaces on homogeneous manifolds of Lie groups and applications, 1993
125 **Masayoshi Nagata,** Theory of commutative fields, 1993
124 **Masahisa Adachi,** Embeddings and immersions, 1993
123 **M. A. Akivis and B. A. Rosenfeld,** Élie Cartan (1869–1951), 1993
122 **Zhang Guan-Hou,** Theory of entire and meromorphic functions: deficient and asymptotic values and singular directions, 1993
121 **I. B. Fesenko and S. V. Vostokov,** Local fields and their extensions: A constructive approach, 1993
120 **Takeyuki Hida and Masuyuki Hitsuda,** Gaussian processes, 1993
119 **M. V. Karasev and V. P. Maslov,** Nonlinear Poisson brackets. Geometry and quantization, 1993
118 **Kenkichi Iwasawa,** Algebraic functions, 1993
117 **Boris Zilber,** Uncountably categorical theories, 1993
116 **G. M. Fel′dman,** Arithmetic of probability distributions, and characterization problems on abelian groups, 1993
115 **Nikolai V. Ivanov,** Subgroups of Teichmüller modular groups, 1992
114 **Seizô Itô,** Diffusion equations, 1992
113 **Michail Zhitomirskiĭ,** Typical singularities of differential 1-forms and Pfaffian equations, 1992
112 **S. A. Lomov,** Introduction to the general theory of singular perturbations, 1992
111 **Simon Gindikin,** Tube domains and the Cauchy problem, 1992
110 **B. V. Shabat,** Introduction to complex analysis Part II. Functions of several variables, 1992
109 **Isao Miyadera,** Nonlinear semigroups, 1992
108 **Takeo Yokonuma,** Tensor spaces and exterior algebra, 1992
107 **B. M. Makarov, M. G. Goluzina, A. A. Lodkin, and A. N. Podkorytov,** Selected problems in real analysis, 1992
106 **G.-C. Wen,** Conformal mappings and boundary value problems, 1992
105 **D. R. Yafaev,** Mathematical scattering theory: General theory, 1992
104 **R. L. Dobrushin, R. Kotecký, and S. Shlosman,** Wulff construction: A global shape from local interaction, 1992
103 **A. K. Tsikh,** Multidimensional residues and their applications, 1992
102 **A. M. Il′in,** Matching of asymptotic expansions of solutions of boundary value problems, 1992
101 **Zhang Zhi-fen, Ding Tong-ren, Huang Wen-zao, and Dong Zhen-xi,** Qualitative theory of differential equations, 1992
100 **V. L. Popov,** Groups, generators, syzygies, and orbits in invariant theory, 1992
99 **Norio Shimakura,** Partial differential operators of elliptic type, 1992
98 **V. A. Vassiliev,** Complements of discriminants of smooth maps: Topology and applications, 1992 (revised edition, 1994)
97 **Itiro Tamura,** Topology of foliations: An introduction, 1992
96 **A. I. Markushevich,** Introduction to the classical theory of Abelian functions, 1992
95 **Guangchang Dong,** Nonlinear partial differential equations of second order, 1991
94 **Yu. S. Il′yashenko,** Finiteness theorems for limit cycles, 1991

(See the AMS catalog for earlier titles)

ISBN 0-8218-0587-8

9 780821 805879