Proceedings of the 1969 Summer Institute on Number Theory: Analytic Number Theory, Diophantine Problems, and Algebraic Number Theory
Held at the State University of New York at Stony Brook
Stony Brook, Long Island, New York
July 7–August 1, 1969

Prepared by the American Mathematical Society
under the National Science Foundation Grant GP–9551

DONALD J. LEWIS
Editor

International Standard Book Number 0–8218–1420–6
Library of Congress Catalog Number 76–125938
Copyright © 1971 by the American Mathematical Society
AMS 1970 Subject Classifications. Primary 10XX, 12XX.
Printed in the United States of America

All rights reserved except those granted to the United States Government
May not be reproduced in any form without permission of the publisher
CANDID CAMERA—
1969 NUMBER THEORY INSTITUTE

J. AX AND A. PFISTER

iii
H. M. STARK  H. P. F. SWINNERTON-DYER  KURT MAHLER

P. T. BATEMAN AND E. GROSSWALD
CONTENTS

Preface ix
Applications of Algebraic Geometry to Number Theory 1
By H. P. F. Swinnerton-Dyer
Abelian Varieties Over Finite Fields 53
By W. C. Waterhouse and J. S. Milne
Introduction aux travaux récents de Dwork 65
By Nicholas M. Katz
The Integral Classical Groups and Their Automorphisms 76
By O. T. O'Meara
Skew-Symmetric Forms for Number Fields 86
By Kenkichi Iwasawa
$K_2$ of Global Fields 87
By B. J. Birch
Class Formations 96
By Yukiyos Kawada
Some Conjectures in Class Field Theory 115
By J. A. Shalika
Extensions of Cyclotomic Theory 123
By Thomas Storer
Reducibility of Lacunary Polynomials 135
By A. Schinzel
Quadratic Forms Over Fields 150
By A. Pfister
A Metamathematical Approach to Some Problems in Number Theory 161
By James Ax
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes on Matijasevič’s Solution of Hilbert’s Tenth Problem</td>
<td>191</td>
</tr>
<tr>
<td>By Julia Robinson</td>
<td></td>
</tr>
<tr>
<td>Effective Methods in Diophantine Problems</td>
<td>195</td>
</tr>
<tr>
<td>By Alan Baker</td>
<td></td>
</tr>
<tr>
<td>On Schanuel’s Conjectures and Skolem’s Method</td>
<td>206</td>
</tr>
<tr>
<td>By James Ax</td>
<td></td>
</tr>
<tr>
<td>On Approximations of Algebraic Numbers by Algebraic Numbers of</td>
<td>213</td>
</tr>
<tr>
<td>Bounded Degree</td>
<td></td>
</tr>
<tr>
<td>By Eduard Wirsing</td>
<td></td>
</tr>
<tr>
<td>Lectures on Transcendental Numbers</td>
<td>248</td>
</tr>
<tr>
<td>By Kurt Mahler</td>
<td></td>
</tr>
<tr>
<td>Mahler’s $T$-Numbers</td>
<td>275</td>
</tr>
<tr>
<td>By Wolfgang M. Schmidt</td>
<td></td>
</tr>
<tr>
<td>Selberg’s Sieve With Weights</td>
<td>287</td>
</tr>
<tr>
<td>By H.-E. Richert</td>
<td></td>
</tr>
<tr>
<td>Sieve Methods</td>
<td>311</td>
</tr>
<tr>
<td>By Atle Selberg</td>
<td></td>
</tr>
<tr>
<td>Density Theorems for the Zeta Function</td>
<td>352</td>
</tr>
<tr>
<td>By Enrico Bombieri</td>
<td></td>
</tr>
<tr>
<td>On Some Recent Results in the Analytical Theory of Numbers</td>
<td>359</td>
</tr>
<tr>
<td>By Paul Turán</td>
<td></td>
</tr>
<tr>
<td>Characterization of the Logarithm as an Additive Function</td>
<td>375</td>
</tr>
<tr>
<td>By Eduard Wirsing</td>
<td></td>
</tr>
<tr>
<td>Some Results Concerning Reciprocity Law and Real Analytic Automorphic Functions</td>
<td>382</td>
</tr>
<tr>
<td>By Tomio Kubota</td>
<td></td>
</tr>
<tr>
<td>Elliptic Curves Over $\mathbb{Q}$: A Progress Report</td>
<td>396</td>
</tr>
<tr>
<td>By B. J. Birch</td>
<td></td>
</tr>
<tr>
<td>Recent Advances in Determining All Complex Quadratic Fields of a Given Class-Number</td>
<td>401</td>
</tr>
<tr>
<td>By H. M. Stark</td>
<td></td>
</tr>
<tr>
<td>Class Number, a Theory of Factorization, and Genera</td>
<td>415</td>
</tr>
<tr>
<td>By Daniel Shanks</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>441</td>
</tr>
<tr>
<td><strong>Subject Index</strong></td>
<td>445</td>
</tr>
</tbody>
</table>
PREFACE

This book is an outgrowth of the American Mathematical Society's Sixteenth Summer Research Institute, which had as its topics algebraic number theory, diophantine problems, and analytic number theory.

The Organizing Committee for the institute consisted of James Ax, Paul T. Bateman, K. Iwasawa, D. J. Lewis (Chairman), and Atle Selberg. The institute was held at the State University of New York at Stony Brook from July 7 to August 1, 1969, and was financed by grants from the National Science Foundation and the New York State Science and Technology Foundation.

During the 1960's a large number of old problems in number theory were solved: some by refinements of known methods, others by the introduction of entirely new methods. One of the purposes of the institute was to acquaint the participants from the various areas of number theory with the important results and methods developed recently, especially in areas other than their own. It is impossible to cover all areas of number theory in a single institute; many of the areas not emphasized at this institute were the subject of other institutes and conferences held here and abroad this past year. In order to survey the achievements of the decade, the Organizing Committee invited sixteen speakers to each give a series of lectures. In addition to the lecture program, there was a seminar program. The list of seminars with speakers and titles are given below; for the most part, the results announced in the seminars will appear elsewhere. This volume consists of the sixteen invited lecture series, plus nine seminar talks which were felt to have been particularly effective surveys. The papers are addressed to a general number theory audience rather than to a group of specialists and are meant to enable a number theorist to become acquainted with important innovations in areas outside his own specialty. It is hoped that this collection of papers will facilitate access to various parts of number theory and foster further development.

In this book the papers are arranged so that those treating related topics or using related techniques appear together. The first few papers treat the role of algebraic geometry in number theory. The highlight of the institute was the series of fourteen lectures by H. P. F. Swinnerton-Dyer on this topic. His paper is an excellent introduction to possible uses of algebraic geometry. The paper by W. Waterhouse and J. Milne treats abelian varieties over finite fields. The paper by N. Katz on p-adic cycles covers the same material as that presented by B. Dwork at the institute, but the presentation is different. Dwork's proof will appear elsewhere.
These papers are followed by a sequence of papers by O. T. O'Meara on automorphisms of the orthogonal group; K. Iwasawa on Jacobians for number fields; B. J. Birch on $K_2$-theory; Y. Kawada on class formations; J. A. Shalika on non-abelian class field theory; T. Storer on cyclotomy; A. Schinzel on reducibility of polynomials; and A. Pfister on the quantitative form of Hilbert's seventeenth problem. These papers treat questions in algebraic number theory or make use of algebraic techniques. Several of these papers serve as an introduction to difficult and sophisticated theory, while others are thorough surveys of a subject.

The first paper by J. Ax demonstrates the relevancy of logic as a tool in number theory. The paper by Julia Robinson is a revision of her lectures which incorporates the recent proof of Ju. V. Matijasevič of Hilbert's tenth problem. This is followed by a report of A. Baker on his effective methods for solving binary equations, methods which at first sight might be judged to be effective from a theoretical point of view but not from a computational one; however, Baker, Davenport, Ellison, and others have demonstrated that with skill these methods can be used very satisfactorily to find all solutions.

The next set of papers deals with transcendental numbers and diophantine approximations. There is a discussion by J. Ax of Schanuel's all-encompassing conjectures, and there is the long-awaited paper by E. Wirsing on approximation of algebraic numbers by algebraic numbers, including some refinements and extensions of those ideas. The paper by K. Mahler is an extensive survey of the theory of transcendental numbers including that by Shidlovsky, and the paper by W. Schmidt discusses his recent work on the existence of Mahler's $T$-numbers.

Next, there are two extensive papers by H.-E. Richert and by Atle Selberg on sieve methods. The paper by Selberg contains proofs of results obtained over several decades but not previously published.

These are followed by papers by E. Bombieri on density theorems for the zeta function; P. Turán on recent results in analytic number theory; and E. Wirsing on characterizing the logarithm as an additive function. The paper by T. Kubota treats the reciprocity law and automorphic functions, and a second paper by Birch treats elliptic curves and modular forms. Finally, there is a paper by H. Stark surveying the class number problem for complex quadratic fields, and there is a paper by D. Shanks on class number and genera.

The photographic insert consists of photos taken of the participants at work and at play by the institute's roving photographer, Carolyn Dana Lewis.

It is an immutable fact of mathematical publishing that there is a substantial period of time between the completion of a manuscript and its appearance in printed form. In a field such as number theory, peopled with energetic and imaginative researchers, it is a foregone conclusion that during this interval a number of important results will be discovered, including answers to problems raised at the institute and in the published proceedings. We note in passing that since these manuscripts were submitted, W. Schmidt has proved the $n$-dimensional Thue-Siegel-Roth theorem; A. Baker and H. Stark have determined the complex quadratic fields with class number two; and E. Bombieri (with P. X. Gallagher and H. Montgomery) has given a simple version of the large sieve.
SEMINARS

ALGEBRAIC NUMBER THEORY

Olga Taussky, Hilbert's Theorem 94.
Richard B. Lakein, Euclid's algorithm in imaginary quartic fields.
H. Heilbronn, Density theorems for cubic fields.
S. Ullom, Groups, rings and cyclotomic fields.
B. Dwork, $p$-adic cycles.
William C. Waterhouse, Abelian varieties over finite fields, I: Classification up to Isogeny.
William C. Waterhouse, Abelian varieties over finite fields, II: Endomorphism rings and isomorphism classes.
J. S. Milne, Relations to the conjectures of Birch and Swinnerton-Dyer.
J. A. Shalika, Representations of $p$-adic groups.
J. A. Shalika, Some conjectures in class field theory.
J. Fresnel, A new definition of $p$-adic $L$-functions.
Koji Doi, On a problem in the theory of automorphic forms.
B. J. Birch, On elliptic curves and modular functions.
Koji Katayama, On some new zeta-functions.

Armand Brumer, Chairman

ANALYTIC NUMBER THEORY

H. L. Montgomery, Mean and large values of Dirichlet polynomials and zeros of $L$-functions.
Lowell Schoenfeld, An improved estimate for the summatory function of the Möbius function.
Karl K. Norton, The distribution of power residues and non-residues.
C. Ryavec, The variation of an additive function.
P. X. Gallagher, A larger sieve.
M. Goldfeld, An application of the large sieve to the Goldbach problem.
L. Ehrenpreis, The zeros of the zeta function on the critical line.
Bruce C. Berndt, On the average order of a class of arithmetical functions.
Wolfgang Schwarz, Weak asymptotic and asymptotic properties of partitions.
S. L. Segal, Tauberian theorems of Landau-Ingham type.
H. M. Stark, An all purpose Tauberian theorem.
E. Bombieri, Density theorems for the zeta function.
P. T. Bateman, Linear relations connecting the imaginary parts of the zeros of the zeta function.
S. Chowla, Some remarks on number theory.

P. T. Bateman, Chairman

CYCLOTOMY, COMBINATORICS, AND ADDITION THEOREMS

Albert Leon Whiteman, Residue Difference Sets.
Thomas Storer, Extensions of Cyclotomic theory.
Joseph B. Muskat, Cyclotomy and evaluation of character sums.
George E. Andrews, Partition identities.
Kenneth B. Stolarsky, Is partition theory inherently quadratic?
Lorne Houten, Plane partitions.
L. Carlitz, Eulerian numbers.
Henry Mann, Addition Theorems.
C. Ryavec, Addition of residue classes modulo $n$.
Robert A. Lee, On the $e$-transform.
E. G. Straus, Some problems concerning sum free and average-free sets.
Calvin T. Long, Factorization of sets of integers.
Emanuel Vegh, Arithmetic progressions of primitive roots of a prime.

A. L. Whiteman and T. Storer, Chairmen

DIOPHANTINE APPROXIMATION AND PROBABILISTIC NUMBER THEORY

William W. Adams, Diophantine approximation in a cubic field.
E. G. Straus, Entire Functions.
W. Philipp, 1. An attempt to unify probabilistic number theory, 2. On limit theorems for additive functions.
P. Szüsz, On the metrical theory of continued fractions.
T. W. Cusick, Diophantine approximation for ternary linear forms.
Wolfgang Schwarz, On the congruence behavior of equivalent power series (a problem of Turán's).
Wolfgang Schwarz, A remark on an asymptotic formula of Renyi.
E. Wirsing, On approximation of algebraic numbers by algebraic numbers of fixed degree.
P. D. T. A. Elliott, The distribution of the values of Dirichlet $L$-series on, and to the left, of the line $\sigma = 1$.
R. T. Bumby, How to double a continued fraction.

D. Cantor and W. Philipp, Chairmen

DIOPHANTINE EQUATIONS

J. Ax, Schanuel's conjecture and decomposable forms by Skolem's methods.
M. Fried, Diophantine equations related to $h(x) - y = a$.
A. Schinzel, An improvement of Runge's Theorem.
L. J. Gerstein, Decompositions of Hermitian forms.
J. M. Ghandi, Fermat's last theorem and generalizations.
O. T. O'Meara, The automorphisms of the orthogonal groups and their congruence subgroups over arithmetic domains.
S. Abhyankar, Some remarks on the Fermat problem.
W. J. Ellison, An easy proof of Waring's problem.
Gordon Pall, Factorization of representations by binary quadratic forms.
L. Carlitz, Gaussian Sums.
John W. Schuck, Counting zeros of polynomials modulo $p^k$ via integration on $p$-adic manifolds.
David Burgess, On the multiplicative group generated by the values of a polynomial.
J. H. H. Chalk and R. A. Smith, Exponential sums and a distribution problem of Mordell.
P. A. Leonard, Polynomial factorization over $GF(p)$.
D. J. Lewis, Simultaneous equations of additive type.

N. C. Ankeny, Chairman
IMAGINARY QUADRATIC FIELDS WITH SMALL CLASS NUMBERS

H. M. Stark, Some historical remarks on class numbers of complex quadratic fields.
P. Weinberger, Complex quadratic fields with class number two and even discriminant.
Carlos J. Moreno, Class number two and related problems.
Larry J. Goldstein, Imaginary quadratic fields with small class numbers.
B. J. Birch, The appropriate field for class invariants.
Daniel Shanks, Class number, a theory of factorization, and genera.

H. M. Stark, Chairman
D. J. Lewis
Ann Arbor, Michigan
AUTHOR INDEX

Italic numbers refer to pages on which a complete reference to a work by the author is given. Roman numbers refer to pages on which a reference is made to a work of the author. For example, under Barsotti would be the page on which a statement like the following occurs: "This theorem was proved earlier by Barsotti [7, Theorem 6] in the following manner..."

Boldface numbers indicate the first page of the articles in this volume.

Albert, A. A., 44, 51
Anfert’e va, E. A., 199, 204
Ankeny, N. C., 287, 299, 303, 304, 308, 311, 351
Artin E., 122
Artin, M., 22, 96, 98–100, 113, 117, 363
Atkin, A. O. L., 93, 398, 399
Ax, James, 157, 161, 203, 204, 206, 212
Baker, Alan, 193, 195, 204, 206, 404, 406, 414
Baldassarri, M., 1, 51
Barban, M. B., 289, 308
Barner, K., 91, 94
Barsotti, 56
Bass, H., 87, 91–93, 94, 395
Bateman, P. T., 297, 298, 307, 308
Bellman, 357
Birch, B. J., 62, 63, 87, 396, 399, 404, 414
Blanksby, P. E., 136
Bohr, 360–362
Bombieri, E., 51, 293, 294, 297, 308, 350, 351, 352, 369
Borel, A., 84
Borevic, Z. I., 94, 207, 212
Brownawell, Dale, 207
Brun, Viggo, 342
Bruner, Armand, 204
Buchstabil, A. A., 299, 303, 305, 307, 308, 311, 342
Bundschuh, P., 199, 204
Capelli, 135
Carlson, 360, 362
Cartier, 56, 104
Cassels, J. W. S., 11, 15, 51, 95, 99, 113, 149, 150, 151, 159
Castelnuovo, 25
Chabauty, C., 38, 206, 210, 211, 212
Chatelet, 10, 15
Chebyshev, 367
Chevally, C., 113
Chow, 8
Coates, J., 202, 204
Cohen, P. M., 79, 84
Conforto, F., 8, 51
Čudakov, N. G., 199, 204
Damerell, M., 397, 400
Davenport, H., 204, 289, 294, 308, 369
Davis, Martin, 161, 192, 194

441
Dedekind, Richard, 427, 440
Deligne, P., 64, 65
Demuskin, S., 110, 113
DeRham, 66
Deuring, Max, 41, 102, 397, 400, 404, 414
Dickson, L. E., 134
Dieudonné, 56, 79
Dirichlet, 198
Douady, A., 108, 113
Dull, M. H., 84
Dwork, B. M., 51, 65, 67, 75, 122
Dyson, F. J., 217, 247
Elliott, P.D.T.A., 370, 437, 440
Ellison, 159
Erdelyi, 392
Erdős, P., 375, 381
Euler, 18, 439
Faber, 250
Feld'man, N. I., 197, 202, 205, 286
Fermat, 31
Fresnel, J., 91, 95
Frobenius, 57, 66
Frolich, A., 95, 99, 113
Fuchs, 67, 71
Gallagher, P. X., 354, 357
Galois, 57
Gauss, C. F., 89, 90, 95, 436, 438, 439, 440
Gelfond, I. M., 122, 195, 196, 198, 199, 250, 406
Giraud, J., 44, 51
Gödel, 161
Godement, R., 112, 120, 122
Gourin, E., 135, 149
Graev, M. I., 122
Grant, K., 106, 113
Grothendieck, A., 22, 23, 51, 59, 64
Guy, M. J. T., 11, 51
Hackel, 250
Halász, G., 353, 357, 358, 362, 364, 369
Halberstam, H., 287, 289, 308, 309, 369
Hardy, G. H., 298, 309
Hardy, 360, 362, 367, 368
Harish-Chandra, 395
Harrison, D. K., 113
Hasse, H., 22, 75, 395
Hecke, 41, 120
Heegner, Kurt, 198, 399, 400, 402–404, 406, 409, 412, 414
Heilbronn, 198, 371
Hermite, 201, 248, 251
Hilbert, 152, 157, 191, 193, 195, 270
Hochschild, G., 112
Hochschild, K., 111, 113
Hock, A., 199, 204
Hodge, 23
Hofmeister, G., 351
Hoheisel, 360
Honda, T., 59, 64
Hooley, 363
Horn, R. A., 297, 308
Hua, L. K., 84
Humphreys, J. E., 79, 84
Hurwitz, 250
Igusa, J.-I., 398, 400
Ingham, 360, 362, 363
Iwashawa, Kenichi, 86, 109, 113
Jacobi, 125
Jacobson, N., 64
Jacobsthal, 125
Jacquet, H., 118, 120, 122
Johnsen, E. C., 134
Jurkat, W. B., 309, 311, 343, 351
Jutila, 370
Kasch, F., 286
Katai, I., 375, 381
Katz, Nocholas M., 65
Kawada, Yukiyosi, 69, 100–107, 109, 110, 113
Kenku, Monsur, 409
Kleiman, S. L., 23, 52
Klimov, N. I., 295, 309
Knapowski, 367
Knuth, Donald E., 440
Koch, 109, 111
Koch, S., 192
Koksma, J. F., 276, 279, 286
Korobov, 360
Kronecker, 41, 44, 136, 409
AUTHOR INDEX

Kubilius, J., 309
Kubota, Tomio, 382, 395
Kuhn, P., 303, 309
Kummer, 390
Kuzmin, 195, 196
Labute, 110, 114
Lagrange, 125
Landau, Edmund, 360–362, 367, 439
Landin, J., 79, 84
Lang, H., 2, 8, 91, 95, 98, 100, 101, 103, 107–109, 114
Lang, S., 52, 64
Langlands, R. P., 117, 118, 120, 122
Lefschetz, S., 23, 73, 75
Legendre, Adrien-Marie, 439, 440
Lehmer, D. H., 136, 415, 428, 440
Lehner, Emma, 415, 433
Lehner, J., 398, 399
Lekkerkerker, 250
Leopold, 203
Leveque, W. J., 214, 218, 247, 279, 286
Levin, B. V., 295, 298, 307, 309
Lindelöf, 360
Lindemann, 206
Linfoot, 198
Linnik, 198, 369, 370, 406
Liouville, 248
Littlewood, J. E., 298, 309, 353, 360, 362, 364, 367, 368, 439
Ljunggren, W., 149
Lucas, E. A., 134, 194
Lyndon, R. C., 110, 114

Maass, 120
Mackey, 79
Mahler, Kurt, 199, 248, 275, 276, 279, 286
Manin, Ju. I., 10, 52
Mathews, G. B., 429, 440
Matijasevič, Ju., 192, 194
Matsumoto, H., 91, 95, 395
Mattuck, A., 23, 52
Messing, W., 65
Miech, R. J., 303, 307, 309
Milne, J. S., 53, 64
Milnor, J., 91, 95, 395
Monsky, P., 66, 75
Montgomery, H. L., 136, 293, 309, 354, 358, 360, 362, 369, 371
Moore, Calvin, 88, 90, 91, 95, 395
Mordell, L. J., 38, 201, 205
Moriya, 103
Motzkin, T. S., 152, 160
Mumford, D., 212

Nagata, 171
Néron, A., 52
Nobile, A., 91, 95

O'Meara, O. T., 76, 79, 85
Oda, T., 56, 64
Ogè, A. P., 400
Oleinikov, 274
Onishi, 287, 299, 303, 304, 308, 311, 351
Oort, F., 64

Pajtechii, I., 122
Pfister, A., 150, 160
Picard, 67, 71, 73
Poincaré, 54
Poitou, G., 111, 114
Pontrjagin, 104, 105
Pracher, K., 295, 309
Putnam, Hilary, 161, 192, 194
Rabinowitsch, 401
Rademacher, H., 342
Rainich, G. Y., 401
Rajwade, A. R., 397, 400
Ramachandra, K., 214, 247
Reid, Constance, 194
Reiner, I., 79, 84, 85
Rényi, A., 303, 309, 369
Ricci, G., 294, 309
Richert, H. –E., 287, 309, 311, 343, 351, 360
Rickart, C. E., 79, 85
Rieger, G., 307, 309
Riemann, 58
Risch, Robert, 207
Robinson, Julia, 161, 191, 192, 194
Robinson, R. M., 152, 160, 194, 194
Rosser, Barkley, 311, 342, 343
Roth, K. F., 199, 218, 247, 287, 309
Ryavec, C., 377, 381
Safarevic, I. R., 94, 107, 111, 114, 207, 212, 428
Samuel, P., 3, 52
Satake, I., 104, 113
Schanuel, 206, 207
Schinzel, A., 135, 149, 297, 298, 309
Schneider, Th., 196, 203, 217, 229, 247, 279, 286
Schoenfeld, L., 360
Schreier, O., 78, 85
Schwarz, W., 298, 309
Segre, B., 10
Selberg, Atle, 287, 303, 309, 311, 351, 384, 395
Serre, J.-P., 64, 93, 95, 96, 98, 99, 101, 103–112, 114, 395, 398, 400
Shalika, J. A., 115, 122
Shanks, Daniel, 368, 415, 440
Shapiro, 122
Shidlovkisi, 251–253, 257, 259–263, 269, 272–274
Shimura, G., 8, 41, 44–46, 49, 51, 52, 59
Sierpinski, W., 309
Skolem, T., 200, 206, 207, 210, 212
Sokolovskij, A. V., 363
Solazzi, R. E., 85
Spiegel, E., 85
Sprindzuk, V. G., 202, 205, 219, 247
Stark, H. M., 198, 205, 401, 404, 412, 414
Stas, W., 363
Steinberg, R., 79, 85, 90, 95
Stemmler, R., 297, 298, 307, 308
Stephens, M. N., 397, 400
Storer, Thomas, 123, 134
Straus, E. G., 149
Swan, R. G., 91, 95
S innerton-Dyer, H. P. F., 1, 2, 51, 52, 62, 63, 399, 400
Takahashi, T., 111, 114
Tamagawa, T., 104, 120, 122
Tanaka, S., 122
Taniyama, Y., 8, 41, 44–46, 52, 59
Tate, J., 2, 23, 52, 56, 59, 60, 62, 63, 64, 75, 87, 89–93, 94, 96, 98–100, 102, 103, 107, 108, 111, 112, 113, 114, 398, 400
Taussky, O., 111
Thue, A., 216, 247
Tits, J., 84
Tschebotarew, N. G., 149
Tsien, C., 107, 160
Turán, P., 353, 358, 359
Uchida, K., 111, 114
Uchiyama, S., 310
van der Waerden, B. L., 78, 85
van Lint, J. H., 309
Verdier, 22
Villamayor, O. E., 91, 95
Vinogradov, A. I., 202, 205, 289, 310, 360
Volkmann, 286
Wan, C.-H., 79, 85
Wang, Y., 298, 310
Washnitzer, G., 75
Waterhouse, W. C., 53, 64
Weber, H., 40, 41, 44, 403, 404, 414
Weierstrass, 250
Weil, Andre, 2, 7, 8, 22, 41, 44, 52, 54, 58, 64, 100, 114, 122, 395, 398, 400
Weinberger, Peter, 409
Whaples, G., 103, 106, 113, 114
Whiteman, A. L., 123, 134
Wirsing, Eduard, A., 213, 276, 278, 279, 286, 310, 375
Witt, 56, 105, 155
Wonenburger, M. J., 79, 85
Yan, S.-J., (Yen Shih-chien), 79, 85
Zassenhaus, H., 85
SUBJECT INDEX

Abelian group, 416, 424
composition, 416
Abelian variety, 8, 53
CM-type, 59
elementary, 54
field of moduli, 44
Frobenius endomorphism, 57
isogeny, 8, 54
Neron-Severi group, 10
ordinary, 62
polarization, 44
weak Mordell-Weil theorem, 29
Weil number, 59
Absolute class field, 40
Absolutely irreducible, 3
Additive function, 375
Algebraic, 248
Algebraic complete fields, 182
Algebraic equivalence, 3
Algebraic extensions of ordered fields, 175
Algebraic groups, 79
Algebraic numbers, 248
approximation by algebraic numbers, 213
F-Liouville, 278
Liouville numbers, 278
Mahler’s classification, 275
S-numbers, 275
T-numbers, 275
U-numbers, 275
Ambiguous forms, 422, 430, 431
Analytical theory of numbers
Bombieri’s conjecture, 369
density hypothesis, 353, 362
density theorems, 361
Lindelöf µ-function, 333, 360
quadratic mean-value, 365
Riemann-Mangoldt theorem, 359
Riemann-Piltz conjecture, 367
ternary Goldbach conjecture, 361
weak Lindelöf conjecture, 364
Anisotropic, 80, 151
Approximation by algebraic numbers, 213
law of large numbers, 229
maximal harmonic subsum, 216
Thue-Siegel-Roth Theorem, 213
Archimedian ordered groups, 174
Arithmetic genus, 10
Automorphism theory of the classical groups, 76
“GE_2-rings”, 80
Hasse domains, 80, 81
integral points, 80
"k-rings with a degree function", 79, 80
local domain, 80, 166
upper half space, 383
Ax-Kochen theorem, 163

Baker's theorem, 298
Basic problem of the general sieve, 314
Bellman's inequality, 354, 357
Binary quadratic forms, 415
Bombieri's conjecture, 369
Brun's sieve, 342
Brun-Titchmarsh type, 293
Buchstab-Rosser sieve, 311, 342

Canonical class, 3
canonical divisor, 3
Canonical cohomology class, 97
Canonical 2-cocycle, 96
Canonical divisor, 3
Cardinality property for ultra products, 162
Chabauty's theorem, 211
Characters, 429
Chevalley groups, 79
C.I.P. neofields, 131–133
CLASNO, 421, 425, 427, 433
Class group, 428

CLASNO, 421, 425, 427, 433
Class field, 40
absolute, 40
canonical 2-cocycle, 96
Class formation, 97
malleable, 105
special, 105
topological, 99
Class number, 401–415
binary quadratic forms, 415
generalized Riemann Hypothesis, 415
Kronecker symbol, 404
real Dirichlet series, 415
theory of factorization, 415, 422

Classical group, 77
general linear group, 76
method of involutions, 79, 80
method of residual spaces, 79, 80, 81
orthogonal group, 77
p-Sylow subgroup, 416, 421, 427, 428
radial automorphisms, 78
special linear group, 76
symplectic group, 77
unitary groups, 77
CM-type, 59
Cohomological dimension, 108
strict cohomological dimension, 108
Complete, 2
Complete additivity, 376
Complete fields, 173
Complex quadratic fields, 401
Dirichlet's formula, 405
Kronecker's limit formula, 409
modular functions, 401, 409, 412
Composition, 416
Composition and reduction, 434
Congruence subgroups, 78
Conjecture of Kummer, 390
Cross-section of a valued field, 185
Curve
arithmetic genus, 10
of genus, 202
complete, 2
differentials of the first kind, 3
geometric genus, 11
infinite descent, 31
m-covering, 32
m-descent, 32
principal divisor, 3
Riemann-Roch theorem for curves, 4
Cycle evanescent, 73
Cycle graph, 426
Cyclotomic classes, 124, 128, 132
periods, 125, 129
Cyclotomic matrix, 124, 132
Cyclotomic numbers, 129, 131–133
Degenerate, 82
Demuškin group, 110
Density hypothesis, 353, 362
Density theorems, 361
Differential 1-forms, 208
Differential field, 207
Differentials of the first kind, 3
Dimension of the sieve, 295
Diophantine problems, 191
elliptic and hyperelliptic equations, 201
exponential, 192
SUBJECT INDEX

Fibonacci number, 192
imaginary quadratic fields with class number, 1, 198
logarithms of algebraic numbers, 195
representation of integers by binary forms, 199
Skolem’s method, 206, 210
universal diophantine equation, 193
Weierstrass elliptic functions, 203
Dirichlet’s formula, 405
Divisor
  algebraic equivalence, 3
  canonical class, 3
  linearly equivalent, 3
  linearly equivalent to zero, 3
  principal, 3
  Dominant factorization, 426
  cycle graph, 426

\[ E_\mathbb{Q}, 396 \]
Effective proof of Thue’s result on
  binary forms, 200
  Eisenstein series, 383
  Hecke operators, 389
Elementary, 54
Elementary statement, 161
Elliptic and hyperelliptic equations, 201
  theorem of Siegel on the equation
    \[ f(x, y) = 0, 202 \]
Elliptic curve
  good, 397
  \[ L_E(S), 398 \]
Elliptic curves with a given conductor, 202
  \[ E_\mathbb{Q}, 396 \]
  Baker’s theorem, 398
  \[ L_{E,S}(S), 397 \]
Equations de Picard-Fuchs, 67
Euler-Legendre method, 439
Exotic symbols, 94
Exponential, 192
  Lindemann’s theorem, 197
  Schanuel’s conjecture, 206
Extension of valuations, 168, 170
  Extremal involution, 81

Fibonacci number, 192
F-Liouville, 278
Field
  algebraic complete, 182
  complete, 173
  complex quadratic, 401
differential field, 207
Hen golian field, 176, 180–182
integral closure, 168
linear disjoint fields, 182
\( p \)-adic regulator, 203
quadratic form, 150
  regular extension, 182
Field of moduli, 44
Fixed space, 82
Formule pour une racine de la fonction
  zeta, 68
Frobenius endomorphism, 57
Full modular group, 402
Functions of Jacobsthal, Jacobi, and
  Lagrange, 125
Fundamental theorem of projective
  geometry, 81, 82, 84
Fundamental lemma, 299

Gauss sums
  conjecture of Kummer, 390
\( GE_2 \)-rings, 80
Gelfond-Schneider theorem, 196
Genera, 415, 428
  characters, 429
  composition and reduction, 434
  principal genus, 430
  pseudosquares, 430
General linear group, 76
General sieve, 311
  basic problem, 314
Generalized metaplectic group, 387
Generalized Riemann Hypothesis, 415
Genus, 4
Geometric genus, 11
Goldbach’s problem, 350
Good elliptic curve, 397
Group
  algebraic, 79
  Archimedean ordered, 174
  Chevalley, 79
class field, 40
  Demuškin, 110
  \[ E_\mathbb{Q}, 396 \]
  Eisenstein series, 383
full modular, 402
generalized metaplectic, 387
pure subgroup, 183

Hasse domains, 80, 81
Hasse set of spots, 81
Hecke operators, 389
Height, 34
Henselian field, 176, 180–182
Henselization of a field, 177
Hilbert’s seventh problem, 196
Hilbert’s problem no. 17, 157
Hilbert’s 10th problem, 161, 191
  elementary statement, 161
  recursively enumerable, 191

Imaginary quadratic fields with class number 1, 198
Immediate extension of a valued field, 178
Infinite descent, 31
Integral classical groups, 77
  congruence subgroups, 78
  integral linear groups, 77
  integral orthogonal groups, 77
Integral closure, 168
Integral linear groups, 77
Integral orthogonal groups, 77
Integral points, 80
Inverse property, 131
Irreducibility theorem, 83
Isogeny, 8, 54
Isotropic, 151

Jacobi identity, 126, 130, 131
Jacobian, 8
Jacobsthal sum, 129

$K_2$, 91
$K_2'$, 88
$K_2F$, 87
$k$ residue sieve, 346
$k$-rings with a degree function, 79, 80

$k$-theory
  canonical cohomology class, 97
  $K_2$, 91
  $K_2'$, 88
  $K_2F$, 87
  norm-residue map, 98
  symbol, 87

Kronecker’s limit formula, 409
  modular functions, 401–409, 412
  Kronecker symbol, 404
$L_E(S)$, 398
$L^*_E(S)$, 397
La fonction zeta, 66
La formule de Picard-Lefschetz, 73
Large sieve, 373
Law of large numbers, 229
Lefschetz fixed point formula, 22
Length of a, 248
Lindelof $\mu$-function, 353, 360
Lindemann’s theorem, 197
Linear disjoint fields, 182
Linear forms in the logarithms, 406
Linearly equivalent, 3
Linearly equivalent to zero, 3
Liouville numbers, 278
Local domain, 80, 166
Logarithms of algebraic numbers, 195
  additive function, 375
  complete additivity, 376
  Gelfond-Schneider theorem, 196
  Hilbert’s seventh problem, 196
  lower bounds for linear forms in logarithms, 197
  linear forms in the logarithms, 406
  problem of Leopoldt, 203
Lower bounds for linear forms in logarithms, 197
Lucas identity, 128
Luroth’s theorem, 5

$m$-covering, 32
$m$-descent, 32
Mahler’s classification, 275
Malleable, 105
Maximal harmonic subsum, 216
Maximum of the absolute values of the conjugates of $\alpha$ relative to $Q$, 257
Method of involutions, 79, 80
  extremal involution, 81
  fundamental theorem of projective geometry, 81, 82, 84
Method of residual spaces, 79, 80, 81
  degenerate, 82
  fixed space, 82
  Hasse set of spots, 81
irreducibility theorem, 83
plane rotation, 82
regular, 82
residual index, 82
residual space, 82
Modular functions, 401, 409, 412
Multiplicative quadratic forms, 154
Neofield, 131
C.I.P. neofields, 131–133
inverse property, 131
Neron-Severi group, 10
Norm isomorphism, 188
Norm residue map, 98
Norm-residue symbol, 97
Nullstellensatz, 162
Numbers represented by $F(p)$, 307
Optimal sieve, 315
Ordinary, 62
Orthogonal group, 77
$p$-adic regulator, 203
$p$-divisible group, 56
$p$-Sylow subgroup, 416, 421, 427, 428
Periods, 125, 129
functions of Jacobsthal, Jacobi, and
Lagrange, 125
Jacobsthal sum, 129
Persistence property for ultra products, 163
Plane rotation, 82
Polarization, 44
Positive definite rational functions, 157
Hilbert’s problem no. 17, 157
Practical sieve, 342
Prime-twin problem, 294
Principal divisor, 3
Principal genus, 430
Problem of Leopoldt, 203
Projective classical groups, 77
Projective congruence groups, 78
Projective integral classical groups, 77
Pseudo Cauchy sequence, 184
Pseudo complete fields, 185
Pseudosquares, 430
Pure subgroup, 183
Quadratic form, 150
anisotropic, 80, 151
isotropic, 151
multiplicative, 154
positive definite rational functions, 157
strictly multiplicative, 154
theorems of Cassels, 150
universal, 151
Radial mean-value, 365
Real automorphisms, 78
Recursively enumerable, 191
Regular, 82
Regular extension, 182
Representation of integers by binary
forms, 199
effective proof of Thue’s result on
binary forms, 200
Thue-Siegel theory, 199
Residual index, 82
Residual space, 82
Riemann hypothesis for function
fields, 22
Riemann Zeta function, 352
Bellman’s inequality, 354, 357
density hypothesis, 353
Lindelöf $\mu$-function, 353, 360
Riemann-Mangoldt theorem, 359
Riemann-Piltz conjecture, 367
Riemann-Roch theorem for curves, 4
genus, 4
S-numbers, 275
Schanuel’s conjecture, 206
Schinzel’s conjecture, 297
Selberg’s sieve with weights, 303
numbers represented by $F(p)$, 307
Sieve, 415, 428
basic problem of the general sieve, 314
Brun’s sieve, 342
Brun-Titchmarsh type, 293
Buchstab-Rosser, 311, 342
dimension of the, 295
fundamental lemma, 299
general, 311
Goldbach’s problem, 350
$k$ residue, 346
large, 373
optimal, 315
practical, 342
prime-twin problem, 294
Schinzel’s conjecture, 297
Selberg’s sieve with weights, 303
twin-prime problem, 350
Skolem’s method, 206, 210
Chabauty’s theorem, 211
differential 1-forms, 208
Special class formation, 105
Special linear group, 76
Strict cohomological dimension, 108
Strictly multiplicative, 154
\(\text{Symb}_0(F)\), 87
\(\text{Symb}^0(F)\), 88
Symbol, 87
exotic, 94
norm-residue, 97
\(\text{Symb}_0(F)\), 87
\(\text{Symb}^0(F)\), 88
tame Hilbert, 88
universal, 87
Symplectic group, 77

\(T\)-numbers, 275
Tame Hilbert symbol, 88
Tate module, 55
\(p\)-divisible group, 56
Ternary Goldbach conjecture, 361
Theorems of Cassels, 150
Theorem of Siegel on the equation
\(f(x,y) = 0, 202\)
curves of genus, 202
eccentric curves with a given conductor, 202
Theory of cyclotomy, 123
cyclotomic classes, 124, 128, 132
cyclotomic matrix, 124, 132
cyclotomic numbers, 129, 131–133
Jacobi identity, 126, 130, 131
Lucas identity, 128
neofield, 131
Theory of factorization, 415, 422
ambiguous forms, 422, 430, 431
dominant factorization, 426
Euler-Legendre method, 439
Thue-Siegel theory, 199
Thue-Siegel-Roth theorem, 213

Topological class formation, 99
Transcendental numbers, 248
length of \(\alpha\), 248
maximum of the absolute values of the conjugates of \(\alpha\) relative to \(\mathbb{Q}\), 257
Twin-prime problem, 350

\(U\)-numbers, 275
Ultra products, 162
cardinality property, 162
Nullstellensatz, 162
persistence property, 163
Uniqueness property of valued fields, 176
Unitary groups, 77
Universal, 151
Universal diophantine equation, 193
Universal symbol, 87
Upper half space, 383

Valuation, 166, 169
algebraic extensions of ordered fields, 175
extension of, 168, 170
local domain, 80, 166
valuation ring, 167
value isomorphism, 170
Valuation ring, 167
Value isomorphism, 170
Valued field
Henselization of a field, 177
cross-section of a valued field, 185
immediate extension of a valued field, 178
norm isomorphism, 188
pseudo Cauchy sequence, 184
pseudo complete fields, 185
uniqueness property of valued fields, 176

Variety
Abelian, 8, 53
absolutely irreducible, 3
height, 34
Jacobian, 8
Lefschetz fixed point formula, 22
Tate module, 55
zeta function, 21, 57, 66
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak Lindelöf conjecture</td>
<td>364</td>
</tr>
<tr>
<td>Weak Mordell-Weil theorem</td>
<td>29</td>
</tr>
<tr>
<td>Weierstrass elliptic functions</td>
<td>203</td>
</tr>
<tr>
<td>Weil conjectures</td>
<td>21</td>
</tr>
<tr>
<td>Weil number</td>
<td>59</td>
</tr>
<tr>
<td>Zeta function</td>
<td>21, 57, 66</td>
</tr>
<tr>
<td>La fonction zeta</td>
<td>66</td>
</tr>
<tr>
<td>$L_E(S)$</td>
<td>398</td>
</tr>
<tr>
<td>Riemann hypothesis for function fields</td>
<td>22</td>
</tr>
<tr>
<td>Weil conjectures</td>
<td>21</td>
</tr>
</tbody>
</table>