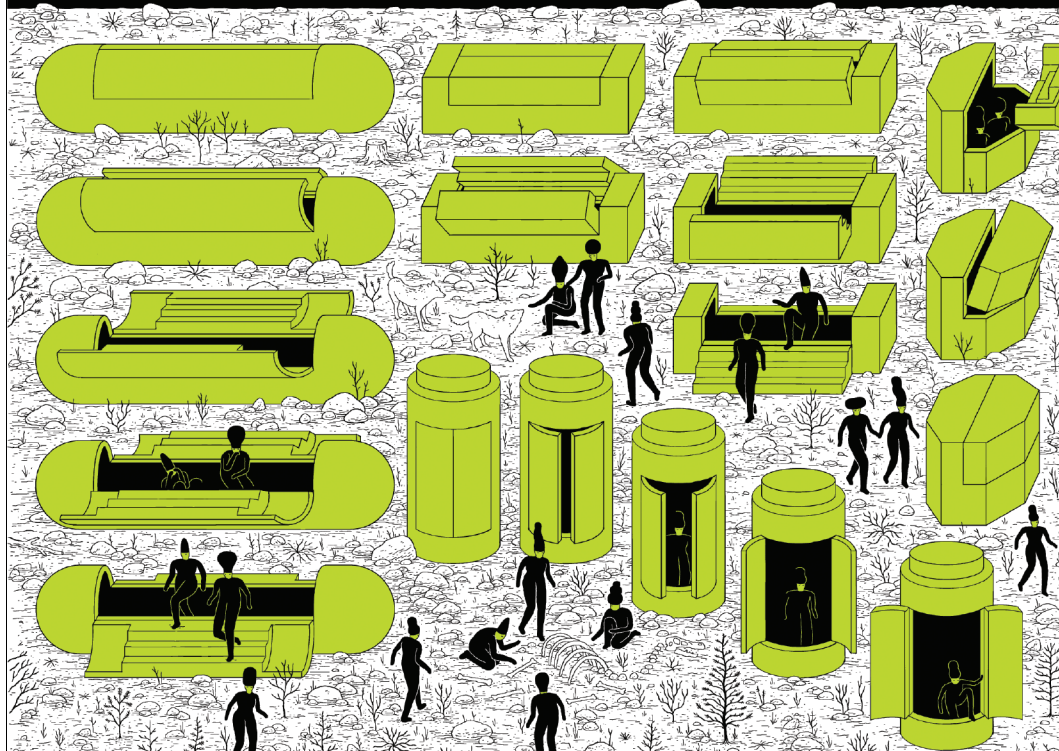
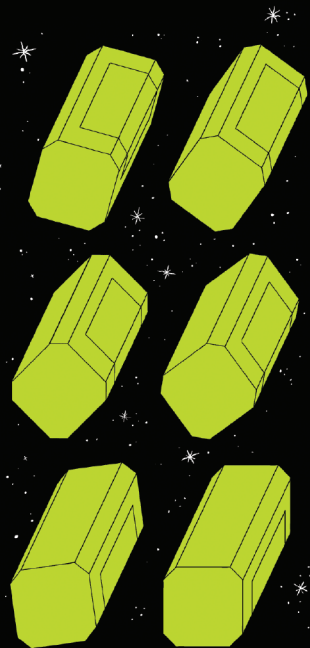


STUDENT MATHEMATICAL LIBRARY
Volume 88

Hilbert's Tenth Problem

An Introduction
to Logic, Number Theory,
and Computability

M. Ram Murty
Brandon Fodden



 **AMS** AMERICAN
MATHEMATICAL
SOCIETY

Hilbert's Tenth Problem

An Introduction
to Logic, Number Theory,
and Computability

STUDENT MATHEMATICAL LIBRARY

Volume 88

Hilbert's Tenth Problem

An Introduction
to Logic, Number Theory,
and Computability

M. Ram Murty

Brandon Fodden



AMERICAN
MATHEMATICAL
SOCIETY

Providence, Rhode Island

Editorial Board

Satyan L. Devadoss
Rosa Orellana

John Stillwell (Chair)
Serge Tabachnikov

2010 *Mathematics Subject Classification*. Primary 11U05, 12L05.

Front cover image by Jesse Jacobs.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-88

Library of Congress Cataloging-in-Publication Data

Names: Murty, Maruti Ram, author. | Fodden, Brandon, 1979– author.

Title: Hilbert's tenth problem : an introduction to logic, number theory, and computability / M. Ram Murty, Brandon Fodden.

Description: Providence, Rhode Island : American Mathematical Society, [2019] | Series: Student mathematical library ; volume 88 | Includes bibliographical references and index.

Identifiers: LCCN 2018061472 | ISBN 9781470443993 (alk. paper)

Subjects: LCSH: Hilbert's tenth problem. | Number theory—Problems, exercises, etc. | Mathematical recreations—Problems, exercises, etc. | Hilbert, David, 1862–1943. | AMS: Number theory – Connections with logic – Decidability. msc | Field theory and polynomials – Connections with logic – Decidability. msc

Classification: LCC QA242 .M8945 2019 | DDC 512.7/4–dc23

LC record available at <https://lcn.loc.gov/2018061472>

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy select pages for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for permission to reuse portions of AMS publication content are handled by the Copyright Clearance Center. For more information, please visit www.ams.org/publications/pubpermissions.

Send requests for translation rights and licensed reprints to reprint-permission@ams.org.

© 2019 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

⊗ 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 <https://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

An algebra of mind, a scheme of sense,
A symbol language without depth or wings,
A power to handle deftly outward things
Are our scant earnings of intelligence.
The Truth is greater and asks deeper ways.

- Sri Aurobindo, "Discoveries of Science II" in *Collected Poems*

Contents

Preface	xi
Acknowledgments	xiii
Introduction	1
Chapter 1. Cantor and Infinity	5
§1.1. Countable Sets	5
§1.2. Uncountable Sets	10
§1.3. The Schröder–Bernstein Theorem	14
Exercises	18
Chapter 2. Axiomatic Set Theory	23
§2.1. The Axioms	23
§2.2. Ordinal Numbers and Well Orderings	28
§2.3. Cardinal Numbers and Cardinal Arithmetic	33
Further Reading	37
Exercises	37
Chapter 3. Elementary Number Theory	41
§3.1. Divisibility	41
§3.2. The Sum of Two Squares	50

§3.3. The Sum of Four Squares	53
§3.4. The Brahmagupta–Pell Equation	55
Further Reading	67
Exercises	67
Chapter 4. Computability and Provability	71
§4.1. Turing Machines	71
§4.2. Recursive Functions	82
§4.3. Gödel’s Completeness Theorems	90
§4.4. Gödel’s Incompleteness Theorems	104
§4.5. Goodstein’s Theorem	114
Further Reading	119
Exercises	120
Chapter 5. Hilbert’s Tenth Problem	123
§5.1. Diophantine Sets and Functions	123
§5.2. The Brahmagupta–Pell Equation Revisited	131
§5.3. The Exponential Function Is Diophantine	137
§5.4. More Diophantine Functions	144
§5.5. The Bounded Universal Quantifier	149
§5.6. Recursive Functions Revisited	155
§5.7. Solution of Hilbert’s Tenth Problem	159
Further Reading	164
Exercises	165
Chapter 6. Applications of Hilbert’s Tenth Problem	167
§6.1. Related Problems	167
§6.2. A Prime Representing Polynomial	171
§6.3. Goldbach’s Conjecture and the Riemann Hypothesis	180
§6.4. The Consistency of Axiomatized Theories	194
Exercises	198

Contents	ix
Chapter 7. Hilbert's Tenth Problem over Number Fields	201
§7.1. Background on Algebraic Number Theory	201
§7.2. Introduction to Zeta Functions and L -functions	212
§7.3. A Brief Overview of Elliptic Curves and Their L -functions	215
§7.4. Nonvanishing of L -functions and Hilbert's Problem	218
Exercises	220
Appendix A. Background Material	223
Bibliography	229
Index	233

Preface

In 1980, the senior author (MRM) had the grand privilege of meeting Sarvadaman Chowla at the Institute for Advanced Study in Princeton, New Jersey. Chowla had written a small book titled *The Riemann Hypothesis and Hilbert's Tenth Problem* in 1965 and so this was an opportunity to ask him about the seemingly strange title and how it came to be. Was there a connection between the two? Chowla replied, "I don't know. These two problems have always fascinated me and so I chose that as the title." He went on to say that the book was largely an inspired work, written in a single night, and it represents his selection of beautiful pearls from number theory. It was not meant to be a textbook but more of an invitation for further study and "to stimulate the reader".

But the fact of the matter is that the two problems *are* related as we discovered only much later in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevič. In fact, many of the famous Hilbert problems are interconnected. This interconnectedness can be used as the focus for mathematical instruction. And it can be done with very few prerequisites. This is the *raison d'être* of this book.

Some of the Hilbert problems such as the Riemann hypothesis (the eighth problem) are still open. The others that have been solved required formidable background and preparation. Hilbert's tenth

problem is different in that a basic introduction to elementary number theory and mathematical logic suffices to understand the proof, and this can be done in a relatively short time. In addition to the grand arrangement of mathematical ideas, Hilbert's tenth problem has a colourful cast of characters, many of them tragic heroes, who pondered deeply regarding the enigma of the human being and the nature of mathematical truth.

Hilbert's tenth problem and its solution represent in microcosm the riddle of human life itself and its meaning. This mélange of philosophical and mathematical conundrums are the mysteries that confront us. In many ways, this book is not meant to be a textbook, but rather an invitation to explore further. As Chowla would say, we hope "to stimulate the reader".

M. Ram Murty and Brandon Fodden

Kingston and Ottawa, Ontario

July 2018

Acknowledgments

This book is based on an upper-level undergraduate course given at Queen's University in Ontario in the winter semester of 2007 by the senior author (MRM). The class consisted of primarily undergraduates, several graduate students, and a few post-doctoral fellows. There were also students from the philosophy department. Given the diverse backgrounds of the students, the mathematical prerequisites were kept to a bare minimum requiring only familiarity with basic calculus and linear algebra. The course covered the contents of the first five chapters by first introducing students to logical notation, then elementary number theory, and gradually to notions of computability and decidability and, finally, the proof of Hilbert's tenth problem. The last two chapters were added later and were culled from graduate seminars conducted since the time the course was first given. They require more advanced background, especially the last chapter. If the student is willing to take some of the background material in those chapters on faith, they will acquire a panoramic view of some recent discoveries and new directions. We feel that this assemblage of subject matter can make an excellent introduction to this fascinating topic and can take the student to the frontiers of current research. We thank Kumar Murty, Hector Pasten, and the referees for their comments on an earlier version of this book. We are grateful to Ina Mette and the American Mathematical Society for taking interest in publishing this book, and to Marcia Almeida at the AMS for much help with preparing the manuscript.

Bibliography

- [AMS] F. E. Browder (ed.), *Mathematical developments arising from Hilbert problems*, Proceedings of Symposia in Pure Mathematics, Vol. XXVIII, American Mathematical Society, Providence, R. I., 1976. MR0419125
- [Ba1] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984. MR781734
- [Ba2] A. Baker, *A comprehensive course in number theory*, Cambridge University Press, Cambridge, 2012. MR2954465
- [BFH] D. Bump, S. Friedberg, and J. Hoffstein, *On some applications of automorphic forms to number theory*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), no. 2, 157–175, DOI 10.1090/S0273-0979-96-00654-4. MR1359575
- [CPZ] G. Cornelissen, T. Pheidas, and K. Zahidi, *Division-ample sets and the Diophantine problem for rings of integers* (English, with English and French summaries), J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR2212121
- [Cr] J. N. Crossley, C. J. Ash, C. J. Brickhill, J. C. Stillwell, and N. H. Williams, *What is mathematical logic?*, Oxford University Press, London-New York, 1972. Oxford Paperbacks University Series, No. 60. MR0414308
- [Dav] H. Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York-Berlin, 1980. Revised by Hugh L. Montgomery. MR606931
- [Da1] M. Davis, *Computability and unsolvability*, McGraw-Hill Series in Information Processing and Computers, McGraw-Hill Book Co., Inc., New York-Toronto-London, 1958. MR0124208
- [Da2] M. Davis, *Hilbert’s tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269, DOI 10.2307/2318447. MR0317916
- [Da3] M. Davis, *On the number of solutions of Diophantine equations*, Proc. Amer. Math. Soc. **35** (1972), 552–554, DOI 10.2307/2037646. MR0304347
- [DMR] M. Davis, Y. Matijasevič, and J. Robinson, *Hilbert’s tenth problem: Diophantine equations: positive aspects of a negative solution*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378. MR0432534

- [Daw] J. W. Dawson Jr., *Logical dilemmas: The life and work of Kurt Gödel*, A K Peters, Ltd., Wellesley, MA, 1997. MR1429389
- [De] R. Dedekind, *Theory of algebraic integers*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1996. Translated from the 1877 French original and with an introduction by John Stillwell. MR1417492
- [D] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220, DOI 10.2307/2040720. MR0360513
- [D1] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236, DOI 10.2307/1998133. MR549163
- [DL] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391, DOI 10.1112/jlms/s2-18.3.385. MR518221
- [DPR] M. Davis, H. Putnam, and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436, DOI 10.2307/1970289. MR0133227
- [Du] A. K. Dutta, *Kuṭṭaka, bhāvanā and cakravāla*, Studies in the history of Indian mathematics, Cult. Hist. Math., vol. 5, Hindustan Book Agency, New Delhi, 2010, pp. 145–199. MR2648498
- [En] H. B. Enderton, *A mathematical introduction to logic*, 2nd ed., Harcourt/Academic Press, Burlington, MA, 2001. MR1801397
- [Fo] B. Fodden, *Diophantine equations and the generalized Riemann hypothesis*, J. Number Theory **131** (2011), no. 9, 1672–1690, DOI 10.1016/j.jnt.2011.01.017. MR2802141
- [Fr] E. Frenkel, *Love and math: The heart of hidden reality*, Basic Books, New York, 2013. MR3155773
- [Ge] S. Gelbart, *An elementary introduction to the Langlands program*, Bull. Amer. Math. Soc. (N.S.) **10** (1984), no. 2, 177–219, DOI 10.1090/S0273-0979-1984-15237-6. MR733692
- [Go] D.C. Goldrei, *Classic set theory for guided independent study*, CRC Press, Boca Raton, FL, 1998.
- [Gra] J. J. Gray, *The Hilbert challenge*, Oxford University Press, Oxford, 2000. MR1828558
- [GT] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547, DOI 10.4007/anal.2008.167.481. MR2415379
- [Ha] P. R. Halmos, *Naive set theory*, Springer-Verlag, New York-Heidelberg, 1974. Reprint of the 1960 edition; Undergraduate Texts in Mathematics. MR0453532
- [HW] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a foreword by Andrew Wiles. MR2445243
- [Haw] S. Hawking (ed.), *God created the integers: The mathematical breakthroughs that changed history*, Running Press, Philadelphia, PA, 2007. Edited, with commentary, by Stephen Hawking. MR2382242
- [Hil02] D. Hilbert, *Mathematical Problems*, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479. MR1557926
- [Ho] R. Hodel, *An Introduction to Mathematical Logic*, Dover Publications, New York, 2013.
- [Hod] A. Hodges, *Alan Turing: the enigma*, The centenary edition, Princeton University Press, Princeton, NJ, 2012. With a foreword by Douglas Hofstadter and a new preface by the author. MR2963548

- [HR] P. Howard and J. E. Rubin, *Consequences of the axiom of choice*, Mathematical Surveys and Monographs, vol. 59, American Mathematical Society, Providence, RI, 1998. With 1 IBM-PC floppy disk (3.5 inch; WD). MR1637107
- [IR] K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York-Berlin, 1982. Revised edition of *Elements of number theory*. MR661047
- [Je] T. Jech, *Set theory: The third millennium edition*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. revised and expanded. MR1940513
- [Jo1] J. P. Jones, *Three universal representations of recursively enumerable sets*, J. Symbolic Logic **43** (1978), no. 2, 335–351, DOI 10.2307/2272832. MR0498049
- [Jo2] J. P. Jones, *Universal Diophantine equation*, J. Symbolic Logic **47** (1982), no. 3, 549–571, DOI 10.2307/2273588. MR666816
- [JSWW] J. P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly **83** (1976), no. 6, 449–464, DOI 10.2307/2318339. MR0414514
- [KP] L. Kirby and J. Paris, *Accessible independence results for Peano arithmetic*, Bull. London Math. Soc. **14** (1982), no. 4, 285–293, DOI 10.1112/blms/14.4.285. MR663480
- [Ku] K. Kunen, *Set theory*, Studies in Logic (London), vol. 34, College Publications, London, 2011. MR2905394
- [LK] C. Leary, and L. Kristiansen, *A friendly introduction to mathematical logic*, Second edition, Milne Library, Genesco, NY, 2015.
- [Ma] Y. V. Matiyasevič, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993. Translated from the 1993 Russian original by the author; With a foreword by Martin Davis. MR1244324
- [Maz] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 1, 14–50, DOI 10.1090/S0273-0979-1993-00414-2. MR1202293
- [MR] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, DOI 10.1007/s00222-010-0252-0. MR2660452
- [Mu] M. R. Murty, *Problems in analytic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008. Readings in Mathematics. MR2376618
- [ME] M. R. Murty and J. Esmonde, *Problems in algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 190, Springer-Verlag, New York, 2005. MR2090972
- [MM1] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L -series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475, DOI 10.2307/2944316. MR1109350
- [MM2] M. R. Murty and V. K. Murty, *Non-vanishing of L -functions and applications*, Progress in Mathematics, vol. 157, Birkhäuser Verlag, Basel, 1997. MR1482805
- [MP] M. R. Murty and H. Pasten, *Elliptic curves, L -functions, and Hilbert's tenth problem*, J. Number Theory **182** (2018), 1–18, DOI 10.1016/j.jnt.2017.07.008. MR3703929
- [MR] M. R. Murty and P. Rath, *Transcendental numbers*, Springer, New York, 2014. MR3134556
- [Ph] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620, DOI 10.2307/2047021. MR962837

- [Po] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42, DOI 10.1007/3-540-45455-1_4. MR2041072
- [SS] H. N. Shapiro and A. Shlapentokh, *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 8, 1113–1122, DOI 10.1002/cpa.3160420805. MR1029120
- [Sh1] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962, DOI 10.1002/cpa.3160420703. MR1008797
- [Sh2] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555, DOI 10.1090/S0002-9947-08-04302-X. MR2386235
- [Sh3] A. Shlapentokh, *Hilbert's tenth problem: Diophantine classes and extensions to global fields*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007. MR2297245
- [Sie] C. L. Siegel, *Zur Theorie der quadratischen Formen* (German), Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1972), 21–46. MR0311578
- [Sil] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210
- [ST] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1171452
- [Sm] C. Smoryński, *Logical number theory I*, Springer-Verlag, Berlin, 1991.
- [Vi] C. Videla, *On Hilbert's tenth problem*. Atas da Xa Escola de Algebra, Vitoria, ES, Brasil Colecao Atas **16** Sociedade Brasileira de Matematica (1989), 95–108.
- [We] A. Weil, *Number theory: An approach through history; From Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, MA, 1984. MR734177
- [Yan] B. H. Yandell, *The honors class: Hilbert's problems and their solvers*, A K Peters, Ltd., Natick, MA, 2002. MR1880187

Index

- L_{PA} , 92
- $LZFC$, 92
- ϵ_0 , 32, 113
- ω , 26
- ω -consistency, 110

- Ackermann function, 85, 88
- Ackermann, W., 85
- adele ring, 211
- adequacy theorem, 99
- admissible, 213
- algebraic integer, 201
- algebraic number, 10, 201
- algebraic number field, 202
- algorithm, 71
- Archimedean valuation, 209
- Aryabhata, 43
- automorphic representation, 213
- axiom of choice, 27, 29, 100
- axiom of existence, 24
- axiom of extensionality, 24
- axiom of infinity, 26
- axiom of regularity, 26
- axiomatized, 106

- Banach, S., 28
- Banach-Tarski paradox, 28
- Bernstein, F., 14
- Bhaskaracharya, 56
- binomial coefficient, 144

- Birch and Swinnerton-Dyer conjecture, 217
- Borel subgroup, 214
- bounded universal quantifier, 149, 153
- Brahmagupta, 56
- Brahmagupta's identity, 51, 52, 57
- Brahmagupta-Pell equation, 55, 66, 131

- canonical interpretation, 99
- Cantor normal form, 33, 117
- Cantor's diagonalization method, 82, 161
- Cantor's pairing function, 7, 128, 156, 168
- Cantor, G., 5, 82
- cardinal, 35
- cardinal addition, 36
- cardinal exponentiation, 36
- cardinal multiplication, 36
- cardinal number, 34
- cardinality, 13
- cartesian product, 7, 36
- Cassels, J. W. S., 220
- Cauchy, A.-L., 204
- chakravala method, 56
- characteristic function, 84, 109
- Chen, J., 181

-
- Chinese remainder theorem, 49, 68, 129
 - Church's thesis, 73
 - Church, A., 73
 - Church–Turing thesis, 73
 - Church–Turing thesis, 159
 - Cohen, P., 28, 37, 101
 - compactness theorem, 102
 - complete arithmetic, 107
 - completeness of Γ , 99
 - complex numbers, 51
 - comprehension schema, 24
 - computable function, 73, 77, 159
 - computable set, 88
 - computably enumerable set, 88, 159
 - conductor, 216
 - congruence, 46
 - conjugate field, 203
 - conjunction, 126
 - consistency of Γ , 98
 - consistency theorem, 98
 - constructible universe, 101
 - continued fraction algorithm, 56
 - continuum hypothesis, 16, 37, 100
 - coprime, 44
 - countable, 6
 - countably infinite, 6
 - cusp forms, 213
 - cuspidal automorphic representation, 213
 - Davis, M., 72, 123, 167
 - de la Vallée Poussin, C., 184
 - decidable property, 182
 - decidable set, 88
 - decimal expansion, 10
 - Dedekind cut, 29, 204, 221
 - Dedekind zeta function, 206
 - Dedekind, R., 14, 203, 205
 - degree, 202
 - Diophantine m -tuple, 69
 - Diophantine equation, 72, 123
 - Diophantine function, 128
 - Diophantine relation, 125
 - Diophantine set, 124, 218
 - Dirichlet approximation theorem, 63
 - Dirichlet, P. G. L., 63, 203, 207
 - discriminant, 208
 - disjunction, 126
 - division algorithm, 41
 - divisor, 42
 - effectively computable, 71
 - Einstein, A., 104
 - elliptic curves, 170, 215
 - empty set, 24
 - Entscheidungsproblem*, 74
 - equivalent valuations, 209
 - Euclid–Mullin sequence, 89
 - Euclidean algorithm, 43
 - Euler product, 185, 206
 - Euler's theorem, 68
 - Euler's totient function, 68
 - Euler, L., 56, 181
 - Euler–Mascheroni constant, 189
 - exponential function, 137
 - expressible relation in PA, 109
 - extension of Peano arithmetic, 106
 - extension theorem, 99
 - factorial function, 83, 145
 - Fermat's last theorem, 205
 - Fermat's little theorem, 48
 - Fermat, P., 56
 - Fibonacci numbers, 67
 - first order language, 91
 - first order logic, 93
 - floor function, 7, 165
 - formula, 92
 - Fraenkel, A., 27
 - Frege, G., 16, 34
 - Frenkel, E., 215
 - Fueter, R., 8
 - Fueter–Pólya theorem, 8
 - function-like formula, 26
 - functional equation, 184
 - fundamental theorem of arithmetic, 45, 186, 205
 - Galois extension, 203
 - Gauss, C. F., 45, 203
 - Gelfond, A., 13
 - general recursive function, 86
 - generalized continuum hypothesis, 37
 - generalized ideal class groups, 210

- generalized Riemann hypothesis, 206
 Gentzen, G., 113
 Gödel number, 108
 Gödel sentence, 111
 Gödel's β function, 129, 130, 156
 Gödel's completeness theorems, 100
 Gödel's first incompleteness theorem, 106
 Gödel's second incompleteness theorem, 112, 195, 197
 Gödel, K., 37, 86
 Gödel, K., 28, 73, 99, 100, 106, 109, 129
 Godement, R., 215
 Goldbach's conjecture, 180
 Goldbach, C., 180
 good reduction, 216
 Goodstein sequence, 114
 Goodstein, R., 115
 greatest common divisor, 42
 Green, B., 164
grossencharacter, 212

 Hadamard, J., 184
 halting problem, 81, 90, 160
 Hardy, G. H., 181
 Harish-Chandra, 214
 Harrington, L., 119
 Hawking, S., 5, 204
 Hecke L -series, 211
 Hecke, E., 206, 211
 Helfgott, H., 181
 Henkin, L., 99
 hereditary expansion, 114
 Hermite, C., 13
 Hilbert problems, 16
 Hilbert's hotel, 17
 Hilbert's tenth problem, 72, 123, 159
 Hilbert's twenty-three problems, 1, 13
 Hilbert, D., 1, 13, 100, 123

 ideal class groups, 210
 ideal theory, 204
 idele group, 211
 inaccessible cardinal, 196

 incompleteness of Γ , 106
 indicator function, 84
 integral basis, 208
 integrally Diophantine, 219
 interpretation of a first order language, 94
 irrational numbers, 9, 12

 Jacquet, H., 215
 Jayadeva, 56
 Jones, J. P., 163, 170–172

 Kirby, L., 118
 Kleene, S., 86
 Kolyvagin, V., 218
 Kronecker, L., 203, 205
 Kronecker–Weber theorem, 219

 Löwenheim, L., 101
 Löwenheim–Skolem theorem, 101
 Lagrange's four square theorem, 53
 Lagrange, J.-L., 53, 56
 lambda calculus, 73
 Landau's classification theorem, 214
 Langlands, R., 212
 language of PA, 92
 language of ZFC, 92
 Levi decomposition, 213
 limit ordinal, 30
 Lindemann, F., 8, 13
 Liouville, J., 13, 202
 listable set, 88
 Littlewood, J. E., 181
 logically valid, 96

 Matiyasevič, Y., 72, 123, 171
 Mazur, B., 217
 minimal polynomial, 202
 minimalization, 86
 Minkowski, H., 208
 model existence theorem, 99
 model of Γ , 96
 modular arithmetic, 46
 modularity conjecture, 216
 modus ponens, 93, 194
 Mordell, L. J., 216
 Mordell–Weil theorem, 216

- non-Archimedean valuation, 209
- nonstandard model, 102
- norm, 206
- normal extension, 203
- order isomorphic, 30
- ordinal, 30, 117
- ordinal addition, 31
- ordinal exponentiation, 32
- ordinal multiplication, 31
- Ostrowski's theorem, 209
- Ostrowski, A., 209
- pairing axiom, 25
- parabolic subgroup, 213
- Paris, J., 118
- parity conjecture, 217
- partial function, 77
- partial recursive function, 86
- partially computable function, 77
- Pastern, H., 220
- Peano axioms, 104
- Pell, J., 56
- Péter, R., 85
- pigeonhole principle, 64, 65
- place, 209
- Pólya, G., 8
- Poonen, B., 219
- power set, 13
- power set axiom, 25
- predecessor function, 84
- prime number, 45
- prime number theorem, 184
- prime representing polynomial, 179
- primitive element, 202
- primitive recursive function, 82
- primitive recursive relation, 85
- projection function, 82
- proof using Γ , 94
- Putnam, H., 72, 123, 127, 147
- Pythagorean triples, 47
- Ramanujan conjecture, 215
- Ramanujan, S., 181
- Ramaré, O., 181
- ramification, 208
- rank, 217
- recursive function, 73, 82, 87, 155
- recursive relation, 85, 109
- recursive set, 88
- recursively enumerable set, 88
- regular cardinals, 196
- relatively prime, 44
- replacement schema, 27
- residue classes, 46
- Ribet, K., 216
- Riemann hypothesis, 184
- Riemann zeta function, 184
- Riemann, B., 184
- Riemann, G. F. B., 203
- right regular representation, 213
- ring of integers, 203
- Robinson, J., 72, 123, 171
- Robinson, R., 85
- Rosser, J. B., 106, 110, 112
- Rubin, K., 217
- Russell's paradox, 17, 93, 96
- Russell, B., 17
- Schneider, T., 13
- Schröder, E., 14
- Schröder–Bernstein theorem, 15, 35
- Selmer, E., 217
- semantic concept, 91
- semidecidable set, 88
- sentence, 92
- Shafarevich–Tate group, 217
- Shapiro, H. N., 183
- Shlapentokh, A., 220
- Siegel, C. L., 170
- Sierpiński, W., 37
- singular cardinals, 196
- Skolem's paradox, 102
- Skolem, T., 101
- soundness theorem, 97
- standard parabolic subgroup, 213
- strongly inaccessible cardinal, 196
- successor cardinal, 35
- successor function, 77, 82
- successor ordinal, 30
- Sunzi Suanjing, 68
- syntactic concept, 91
- Taniyama–Shimura conjecture, 216
- Tao, T., 164
- Tarski, A., 28, 94
- Tate's thesis, 210

- term, 92
- ternary Goldbach problem, 181
- theorem listing algorithm, 194
- total function, 77, 155
- total ordering, 29
- totally real field, 207
- totient function, 68
- transcendental number, 12, 201
- transitive set, 29
- trichotomy law for cardinals, 35
- trivial valuation, 209
- truth in an interpretation, 95
- Turing machine, 73, 75, 120
- Turing's thesis, 73
- Turing, A., 73, 81, 171
- twin prime conjecture, 198
- twin primes, 198

- uncountable, 6
- union set axiom, 25
- unipotent radical, 213
- unique factorization theorem, 45, 205
- universal Turing machine, 171
- universality theorem, 162

- valuation, 208, 211
- Vinogradov, I. M., 181
- von Mangoldt function, 186
- von Neumann assignment, 34
- von Neumann, J., 30

- weakly inaccessible cardinals, 196
- Weil, A., 216
- well-ordering, 29
- Wiles, A., 216
- Wilson's theorem, 48, 147, 166, 172

- Zermelo, E., 27

Selected Published Titles in This Series

- 88 **M. Ram Murty and Brandon Fodden**, Hilbert's Tenth Problem, 2019
- 87 **Matthew Katz and Jan Reimann**, An Introduction to Ramsey Theory, 2018
- 86 **Peter Frankl and Norihide Tokushige**, Extremal Problems for Finite Sets, 2018
- 85 **Joel H. Shapiro**, Volterra Adventures, 2018
- 84 **Paul Pollack**, A Conversational Introduction to Algebraic Number Theory, 2017
- 83 **Thomas R. Shemanske**, Modern Cryptography and Elliptic Curves, 2017
- 82 **A. R. Wadsworth**, Problems in Abstract Algebra, 2017
- 81 **Vaughn Climenhaga and Anatole Katok**, From Groups to Geometry and Back, 2017
- 80 **Matt DeVos and Deborah A. Kent**, Game Theory, 2016
- 79 **Kristopher Tapp**, Matrix Groups for Undergraduates, Second Edition, 2016
- 78 **Gail S. Nelson**, A User-Friendly Introduction to Lebesgue Measure and Integration, 2015
- 77 **Wolfgang Kühnel**, Differential Geometry: Curves — Surfaces — Manifolds, Third Edition, 2015
- 76 **John Roe**, Winding Around, 2015
- 75 **Ida Kantor, Jiří Matoušek, and Robert Šámal**, Mathematics++, 2015
- 74 **Mohamed Elhamdadi and Sam Nelson**, Quandles, 2015
- 73 **Bruce M. Landman and Aaron Robertson**, Ramsey Theory on the Integers, Second Edition, 2014
- 72 **Mark Kot**, A First Course in the Calculus of Variations, 2014
- 71 **Joel Spencer**, Asymptopia, 2014
- 70 **Lasse Rempe-Gillen and Rebecca Waldecker**, Primality Testing for Beginners, 2014
- 69 **Mark Levi**, Classical Mechanics with Calculus of Variations and Optimal Control, 2014
- 68 **Samuel S. Wagstaff, Jr.**, The Joy of Factoring, 2013
- 67 **Emily H. Moore and Harriet S. Pollatsek**, Difference Sets, 2013
- 66 **Thomas Garrity, Richard Belshoff, Lynette Boos, Ryan Brown, Carl Lienert, David Murphy, Junalyn Navarra-Madsen, Pedro Poitevin, Shawn Robinson, Brian Snyder, and Caryn Werner**, Algebraic Geometry, 2013

For a complete list of titles in this series, visit the
AMS Bookstore at www.ams.org/bookstore/stmlseries/.

Hilbert's tenth problem is one of 23 problems proposed by David Hilbert in 1900 at the International Congress of Mathematicians in Paris. These problems gave focus for the exponential development of mathematical thought over the following century. The tenth problem asked for a general algorithm to determine if a given Diophantine equation has a solution in integers. It was finally resolved in a series of papers written by Julia Robinson, Martin Davis, Hilary Putnam, and finally Yuri Matiyasevich in 1970. They showed that no such algorithm exists.

This book is an exposition of this remarkable achievement. Often, the solution to a famous problem involves formidable background. Surprisingly, the solution of Hilbert's tenth problem does not. What is needed is only some elementary number theory and rudimentary logic. In this book, the authors present the complete proof along with the romantic history that goes with it. Along the way, the reader is introduced to Cantor's transfinite numbers, axiomatic set theory, Turing machines, and Gödel's incompleteness theorems.

Copious exercises are included at the end of each chapter to guide the student gently on this ascent. For the advanced student, the final chapter highlights recent developments and suggests future directions. The book is suitable for undergraduates and graduate students. It is essentially self-contained.

ISBN 978-1-4704-4399-3



9 781470 443993

STML/88



For additional information
and updates on this book, visit

www.ams.org/bookpages/stml-88

