Hilbert’s Tenth Problem

An Introduction to Logic, Number Theory, and Computability
Hilbert’s Tenth Problem

An Introduction to Logic, Number Theory, and Computability

M. Ram Murty
Brandon Fodden
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

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
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


Bibliography


Index

$L_{PA}$, 92
$L_{ZFC}$, 92
$\varepsilon_0$, 52, 113
$\omega$, 20
$\omega$-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, 20
axiomatized, 106

Banach, S., 28
Banach–Tarski paradox, 28
Bernstein, F., 14
Bhaskarakarya, 56
binomial coefficient, 144

Birch and Swinnerton-Dyer conjecture, 217
Borel subgroup, 213
bounded universal quantifier, 149
Brahmagupta, 56
Brahmagupta’s identity, 51, 52, 57
Brahmagupta–Pell equation, 55
66, 131

canonical interpretation, 90
Cantor normal form, 83, 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, 50
characteristic function, 84, 109
Chen, J., 181
Index

Chinese remainder theorem, 49, 68
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 $\Gamma$, 99
complex numbers, 41
comprehension schema, 23
computable function, 73, 77, 159
computable set, 88
computably enumerable set, 88, 159
discriminant, 208
disjunction, 126
division algorithm, 11
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., 86, 181
Euler–Mascheroni constant, 180
exponential function, 137
expressible relation in PA, 109
extension of Peano arithmetic, 100
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, 105
formula, 92
Fraenkel, A., 27
Frege, G., 16, 31
Frenkel, E., 215
Fueter, R., 8
Fueter–Pólya theorem, 5
function-like formula, 26
functional equation, 184
fundamental theorem of arithmetic, 184
Galois extension, 203
Gauss, C. F., 45
Gelfond, A., 13
general recursive function, 86
generalized continuum hypothesis, 57
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
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
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
Hilbert’s twenty-three problems, 11
Hilbert, D., 113, 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, 93
irrational numbers, 9, 12
Jacquet, H., 215
Jayadeva, 156
Jones, J. P., 163, 170, 172
Kirby, L., 118
Kleene, S., 86
Kolyvagin, V., 218
Kronecker, L., 214, 206
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
Langlands 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., 53, 56
listable set, 88
Littlewood, J. E., 181
logically valid, 96
Matiyasevič, Y., 123, 171
Mazur, B., 217
minimal polynomial, 202
minimalization, 86
Minkowski, H., 208
model existence theorem, 99
model of Γ, 98
modular arithmetic, 16
modularity conjecture, 216
modus ponens, 93, 194
Mordell, L. J., 216
Mordell–Weil theorem, 210
Index

non-Archimedean valuation, 209
nonstandard model, 109
norm, 206
normal extension, 203

order isomorphic, 50
ordinal, 109, 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, 85
partially computable function, 77
Pasten, 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, 183
prime representing polynomial, 179
primitive element, 202
primitive recursive function, 82
primitive recursive relation, 85
projection function, 82
proof using Γ, 94
Putnam, H., 125, 124, 147
Pythagorean triples, 68

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, 43
replacement schema, 27
residue classes, 46
Ribet, K., 210
Riemann hypothesis, 183
Riemann zeta function, 183
Riemann, B., 123
Riemann, G. F. B., 203
right regular representation, 213
ring of integers, 203
Robinson, J., 125, 147
Robinson, R., 85
Rosser, J. B., 106, 110, 112
Rubin, K., 219
Russell’s paradox, 17, 93, 96
Russell, B., 17
Schneider, T., 117
Schröder, E., 114
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, 114
successor cardinal, 35
successor function, 77, 82
successor ordinal, 40
Sunzi Suanjing, 68
syntactic concept, 91

Taniyama–Shimura conjecture, 216
Tao, T., 107
Tarski, A., 28, 04
Tate’s thesis, 210
**Index**

<table>
<thead>
<tr>
<th>Term / Concept</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>term</td>
<td>92</td>
</tr>
<tr>
<td>ternary Goldbach problem</td>
<td>181</td>
</tr>
<tr>
<td>theorem listing algorithm</td>
<td>194</td>
</tr>
<tr>
<td>total function</td>
<td>77, 155</td>
</tr>
<tr>
<td>total ordering</td>
<td>29</td>
</tr>
<tr>
<td>totally real field</td>
<td>207</td>
</tr>
<tr>
<td>totient function</td>
<td>68</td>
</tr>
<tr>
<td>transcendental number</td>
<td>12, 201</td>
</tr>
<tr>
<td>transitive set</td>
<td>29</td>
</tr>
<tr>
<td>trichotomy law for cardinals</td>
<td>35</td>
</tr>
<tr>
<td>trivial valuation</td>
<td>269</td>
</tr>
<tr>
<td>truth in an interpretation</td>
<td>95</td>
</tr>
<tr>
<td>Turing machine</td>
<td>73, 75, 120</td>
</tr>
<tr>
<td>Turing’s thesis</td>
<td>73</td>
</tr>
<tr>
<td>Turing, A.</td>
<td>73, 81, 171</td>
</tr>
<tr>
<td>twin prime conjecture</td>
<td>198</td>
</tr>
<tr>
<td>twin primes</td>
<td>198</td>
</tr>
<tr>
<td>uncountable</td>
<td>6</td>
</tr>
<tr>
<td>union set axiom</td>
<td>25</td>
</tr>
<tr>
<td>unipotent radical</td>
<td>213</td>
</tr>
<tr>
<td>unique factorization theorem</td>
<td>45, 205</td>
</tr>
<tr>
<td>valuation</td>
<td>208, 211</td>
</tr>
<tr>
<td>Vinogradov, I. M.</td>
<td>181</td>
</tr>
<tr>
<td>von Mangoldt function</td>
<td>186</td>
</tr>
<tr>
<td>von Neumann assignment</td>
<td>34</td>
</tr>
<tr>
<td>von Neumann, J.</td>
<td>30</td>
</tr>
<tr>
<td>weakly inaccessible cardinals</td>
<td>196</td>
</tr>
<tr>
<td>Weil, A.</td>
<td>216</td>
</tr>
<tr>
<td>well-ordering</td>
<td>29</td>
</tr>
<tr>
<td>Wiles, A.</td>
<td>216</td>
</tr>
<tr>
<td>Wilson’s theorem</td>
<td>18, 117, 160, 172</td>
</tr>
<tr>
<td>Zermelo, E.</td>
<td>27</td>
</tr>
</tbody>
</table>
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
78 Gail S. Nelson, A User-Friendly Introduction to Lebesgue Measure and Integration, 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
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.