# Contents


**1 The Claimant, the Readers, and the Crowd** . . . . . 1
1.1 The News . . . . . 1
1.2 The Paper and First Post . . . . . 2
1.3 My Snap-Doubt and Comment . . . . . 3
1.4 Comments and Comments and Comments . . . . . 4
1.5 Back to the Future . . . . . 6
1.6 The Group . . . . . 8
1.7 Internet Non-resistance . . . . . 9
1.8 Company... . . . . 11
1.9 ...And a Crowd . . . . . 12
1.10 The Issues Crystallize . . . . . 13
1.11 The Falling Action . . . . . 14
1.12 What Did We Learn? . . . . . 16
1.13 Notes and Links . . . . . 17

**2 Kenneth Iverson: Notation and Thinking** . . . . . 19
2.1 Good Notation . . . . . 20
2.2 Good Notation? . . . . . 22
2.3 Open Problems . . . . . 23
2.4 Notes and Links . . . . . 23

**3 Edmund Hillary: Proofs and Mountain Climbing** . . . . . 25
3.1 A Disclaimer . . . . . 25
3.2 Climbing . . . . . 25
3.3 Solving . . . . . 26
3.4 Open Problems . . . . . 27
3.5 Notes and Links . . . . . 28

**4 Leonardo da Vinci: Proofs as Art** . . . . . 29
4.1 Studying Great Art . . . . . 29
4.2 Studying Great Proofs . . . . . 30
4.3 Some Great Proofs . . . . . 31
4.4 What Can One Learn from This Study? . . . . . 31
4.5 Open Problems . . . . . 33
4.6 Notes and Links . . . . . 34




Bibliografische Informationen
http://d-nb.info/1042340420

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

**5 Michael Atiyah: The Role of Proof** . . . . . 35
5.1 Does Any Proof Matter? . . . . . 36
5.2 Does a Proof of $P \neq NP$ Matter? . . . . . 36
5.3 Open Problems . . . . . 37
5.4 Notes and Links . . . . . 37

**6 Subhash Khot: Unique Games Conjecture** . . . . . 39
6.1 Act I: The Unique Games Conjecture . . . . . 39
6.2 Act II: The Conjecture's Applications . . . . . 41
6.3 Act III: Is It True? . . . . . 41
6.4 A Comment on Expanders . . . . . 42
6.5 Open Problems . . . . . 43
6.6 Notes and Links . . . . . 43

**7 Arno van den Essen: An Amazing Conjecture** . . . . . 45
7.1 The Jacobian Conjecture . . . . . 45
7.2 JC Approaches . . . . . 47
7.3 Amazing Conjectures . . . . . 48
7.4 Open Problems . . . . . 49
7.5 Notes and Links . . . . . 50

**8 Richard Hamilton: Group Efforts** . . . . . 51
8.1 Fermat's Last Theorem . . . . . 51
8.2 Applying the Idea for a Partial Result . . . . . 52
8.3 Poincaré Conjecture . . . . . 53
8.4 Unique Games Conjecture . . . . . 54
8.5 Open Problems . . . . . 54
8.6 Notes and Links . . . . . 54

**9 Grigori Perelman: A New Clay Problem** . . . . . 57
9.1 Problems . . . . . 58
9.2 Open Problems . . . . . 58
9.3 Notes and Links . . . . . 59

**10 Eric Allender: Solvable Groups** . . . . . 61
10.1 Allender on the Permanent . . . . . 62
10.2 A Result to Dream of . . . . . 62
10.3 $\mathcal{SOLVE}$ . . . . . 63
10.4 Open Problems . . . . . 63
10.5 Notes and Links . . . . . 64

**11 Enrico Bombieri: On Intuition** . . . . . 65
11.1 Number Theory . . . . . 66
11.2 Geometry . . . . . 67
11.3 Groups . . . . . 67
11.4 Reid's Proof . . . . . 67
11.5 Complexity Theory . . . . . 69
11.6 Open Problems . . . . . 69
11.7 Notes and Links . . . . . 69

**12 Fred Hennie: Lower Bounds** . . . . . 71
12.1 The Models . . . . . 71
12.2 Hennie's Result . . . . . 72
12.3 Since Hennie . . . . . 72
12.4 Toward Even Stronger Bounds . . . . . 73
12.5 Open Problems . . . . . 74
12.6 Notes and Links . . . . . 74

**13 Volker Strassen: Amazing Results** . . . . . 75
13.1 Fast Matrix Product . . . . . 75
13.2 All for the Price of One . . . . . 76
13.3 Finding Triangles . . . . . 76
13.4 One Bit, Two Bits, Three Bits, $n$ Bits . . . . . 77
13.5 Open Problems . . . . . 77
13.6 Notes and Links . . . . . 77

**14 Adam Smith: Dumb Channels** . . . . . 79
14.1 Computationally Limited Channels . . . . . 80
14.2 The New Results . . . . . 80
14.3 Open Problems . . . . . 81
14.4 Notes and Links . . . . . 81

**15 Georg Cantor: Diagonal Method** . . . . . 83
15.1 Proofs . . . . . 83
15.2 A Variant of the Classic Proof . . . . . 84
15.3 A Probability-Based Proof . . . . . 85
15.4 Open Problems . . . . . 86
15.5 Notes and Links . . . . . 86

**16 Raymond Smullyan: The Reals Are Uncountable** . . . . . 87
16.1 Alice and Bob Play Some Games . . . . . 88
16.2 Let's Look at Bob's Strategies . . . . . 89
16.3 Is Diagonalization Cheating? . . . . . 89
16.4 Can We Fix This? . . . . . 90
16.5 Open Problems . . . . . 90
16.6 Notes and Links . . . . . 91

**17 William Tutte: Flow Problems** . . . . . 93
17.1 Flow Conjectures . . . . . 94
17.2 Tensor Trick . . . . . 95
17.3 Sketch of Proof . . . . . 95
17.4 Open Problems . . . . . 97
17.5 Notes and Links . . . . . 97

**18 Basil Rathbone: Writing a Major Result** . . . . . 99
18.1 My Suggestions . . . . . 99
18.2 Open Problems . . . . . 102
18.3 Notes and Links . . . . . 103

**19 Elwyn Berlekamp: Dots and Boxes** . . . . . 105
19.1 A Colorful Game . . . . . 106
19.2 Packing Graphs . . . . . 107
19.3 Open Problems . . . . . 108
19.4 Notes and Links . . . . . 108

**20 David Johnson: Galactic Algorithms** . . . . . 109
20.1 Galactic Algorithms . . . . . 109
20.2 Some Examples . . . . . 110
20.3 Open Problems . . . . . 111
20.4 Notes and Links . . . . . 112

**21 Warren Hirsch: Guessing the Truth** . . . . . 113
21.1 Guesses and the Truth . . . . . 113
21.2 Open Problems . . . . . 116
21.3 Notes and Links . . . . . 116

**22 Shimon Even: A Promise Problem** . . . . . 119
22.1 The Promise Problem . . . . . 120
22.2 The Complexity of TWOPATHS . . . . . 121
22.3 Open Problems . . . . . 122
22.4 Notes and Links . . . . . 122

**23 Matei David: Improving Noam Nisan's Generator** . . . . . 123
23.1 The Nisan Generator . . . . . 124
23.2 Read It Again? . . . . . 124
23.3 Open Problems . . . . . 125
23.4 Notes and Links . . . . . 125

**24 Ryan Williams: A New Lower Bound** . . . . . 127
24.1 The Result . . . . . 127
24.2 The Proof Schema . . . . . 127
24.3 Open Problems . . . . . 128
24.4 Notes and Links . . . . . 128

**25 Joel Seiferas: More on the New Lower Bound** . . . . . 129
25.1 The Landscape of Ignorance . . . . . 130
25.2 Outline of the Proof . . . . . 130
25.3 Open Problems . . . . . 132
25.4 Notes and Links . . . . . 133

**26 Victor Klee: Big Results** . . . . . 135
26.1 Three Big Results . . . . . 135
26.2 One More . . . . . 137
26.3 Open Problems . . . . . 138
26.4 Notes and Links . . . . . 138

**27 George Dantzig: Equations, Equations, and Equations** . . . . . 139
27.1 Linear Equations . . . . . 140
27.2 Linear Equations over Non-negative Numbers . . . . . 140
27.3 Linear Equations over Natural Numbers . . . . . 141
27.4 Programming IP . . . . . 142
27.5 Programming Tricks . . . . . 143
27.6 Limits on the Power of IP . . . . . 144
27.7 Complexity Theory . . . . . 144
27.8 Conventional Wisdom . . . . . 145
27.9 Open Problems . . . . . 145
27.10 Notes and Links . . . . . 145

**28 Srinivasa Ramanujan: The Role of Amateurs** . . . . . 147
28.1 Who Is an Amateur? . . . . . 148
28.2 Some Results of Amateurs . . . . . 148
28.3 Problem Statements . . . . . 149
28.4 Can Amateurs Help? . . . . . 150
28.5 Open Problems . . . . . 150
28.6 Notes and Links . . . . . 151

**29 John Rhodes: Approaches to Problems** . . . . . 153
29.1 Approaches Used by Mathematics and Theory . . . . . 153
29.2 Approaches Unique to Mathematics? . . . . . 154
29.3 Open Problems . . . . . 156
29.4 Notes and Links . . . . . 156

**30 John Nash: Connections** . . . . . 159
30.1 Connections . . . . . 160
30.2 The Connection . . . . . 161
30.3 Open Problems . . . . . 161
30.4 Notes and Links . . . . . 162

**31 Chee Yap: Computing Digits of $\pi$** . . . . . 163
31.1 The BBP Algorithm . . . . . 164
31.2 The BBP Algorithm Is Not an Algorithm . . . . . 164
31.3 Yap's Theorem . . . . . 164
31.4 Open Problems . . . . . 165
31.5 Notes and Links . . . . . 165

**32 Henri Lebesgue: Projections Are Tricky** . . . . . 167
32.1 Let's Be Nice . . . . . 168
32.2 Projections . . . . . 168
32.3 Shadows and Slices . . . . . 169
32.4 Strassen's Complexity Measure . . . . . 169
32.5 How the Measure Plays Nice . . . . . 170
32.6 The Problem with Projections . . . . . 171
32.7 Endgame? . . . . . 172

32.8 Open Problems . . . 173
32.9 Notes and Links . . . 173

**33 Nina Balcan: A New Model of Complexity** . . . 175
33.1 Classic Complexity Models . . . 175
33.2 A New Model . . . 176
33.3 Application to Clustering . . . 176
33.4 Open Problems . . . 177
33.5 Notes and Links . . . 178

**34 Sam Buss: Bounded Logic** . . . 179
34.1 A Problem with First-Order Logic . . . 180
34.2 Open Problems . . . 181
34.3 Notes and Links . . . 181

**35 Anton Klyachko: Car Crashes** . . . 183
35.1 Car Crash Theorem . . . 184
35.2 A Proof Sketch . . . 185
35.3 Another View . . . 186
35.4 Why Is It Important? . . . 187
35.5 The Application . . . 187
35.6 Open Problems . . . 188
35.7 Notes and Links . . . 188

**36 Bernard Chazelle: Natural Algorithms** . . . 189
36.1 Natural . . . 190
36.2 Form of Bernard's Talk . . . 191
36.3 Content of the Talk . . . 191
36.4 Open Problems . . . 192
36.5 Notes and Links . . . 192

**37 Thomas Jech: The Axiom of Choice** . . . 195
37.1 Finite Choice . . . 195
37.2 The General Theorem . . . 196
37.3 Open Problems . . . 197
37.4 Notes and Links . . . 197

**38 Alfonso Bedoya: Definitions, Definitions, and Definitions** . . . 199
38.1 Definitions . . . 199
38.2 Mathematical Definitions . . . 200
38.3 Computational Definitions . . . 201
38.4 Justification of Definitions . . . 202
38.5 Open Problems . . . 203
38.6 Notes and Links . . . 203

**39 Hartley Rogers: Complexity Classes** . . . 205
39.1 The Big Three Ideas . . . 206
39.2 How Many Classes Are There? . . . 207

39.3 Special Classes . . . 208
39.4 Properties of Complexity Classes . . . 209
39.5 Open Problems . . . 209
39.6 Notes and Links . . . 210

**40 Ron Fagin: Second-Order Logic** . . . 211
40.1 Courcelle's Theorem . . . 211
40.2 Treewidth . . . 212
40.3 MSO . . . 212
40.4 Proof Idea . . . 213
40.5 Open Problems . . . 214
40.6 Notes and Links . . . 214

**41 Daniel Lokshtanov: Knapsack Problem** . . . 215
41.1 The Method . . . 216
41.2 Constant Term Method . . . 217
41.3 Applications of CEM . . . 217
41.4 A Lemma . . . 218
41.5 Open Problems . . . 219
41.6 Notes and Links . . . 219

**42 Albert Einstein: Beyond Polynomial Equations** . . . 221
42.1 Polynomials Plus . . . 222
42.2 Polynomials Plus Plus . . . 223
42.3 Gravity Lenses . . . 224
42.4 Open Problems . . . 224
42.5 Notes and Links . . . 225

**43 Denis Thérien: Solvable Groups** . . . 227
43.1 Equations over a Group . . . 228
43.2 No Fundamental Theorem of Groups . . . 228
43.3 A Partial Fundamental Theorem . . . 229
43.4 Toward the General Case . . . 229
43.5 Universal Groups . . . 230
43.6 Open Problems . . . 231
43.7 Notes and Links . . . 231

**44 Andreas Björklund: Hamiltonian Cycles** . . . 233
44.1 The Result . . . 233
44.2 An Overview of the Proof . . . 234
44.3 Proof Summary . . . 235
44.4 Open Problems . . . 236
44.5 Notes and Links . . . 236

**45 David Hilbert: The Nullstellensatz** . . . 237
45.1 Hilbert's Nullstellensatz . . . 238
45.2 An Application . . . 238
45.3 How to Express Injective as an Existential Formula . . . 239

45.4 Open Problems . . . 240
45.5 Notes and Links . . . 240

**46 John Hopcroft: Thinking out of the Box** . . . 241
46.1 A National Meeting? . . . 242
46.2 Federated Conferences . . . 242
46.3 Open Problems . . . 243
46.4 Notes and Links . . . 243

**47 Dick Karp: The Polynomial Hierarchy** . . . 245
47.1 Kannan's Theorem . . . 245
47.2 Kannan's Proof . . . 246
47.3 Kannan's Proof—Can We Do Better? . . . 246
47.4 How to Compare Circuits Fast . . . 247
47.5 Open Problems . . . 248
47.6 Notes and Links . . . 248

**48 Nick Howgrave-Graham and Antoine Joux: Attacking the Knapsack Problem** . . . 249
48.1 The Problem . . . 250
48.2 The New Algorithm . . . 251
48.3 The Schroeppel and Shamir Algorithm . . . 251
48.4 Add Hashing . . . 252
48.5 Open Problems . . . 253
48.6 Notes and Links . . . 253

**49 Hedy Lamarr: The Role of Amateurs** . . . 255
49.1 Spread Spectrum . . . 255
49.2 Why Did She Fail? . . . 256
49.3 Open Problems . . . 257
49.4 Notes and Links . . . 257

**50 Nicolas Courtois: The Linearization Method** . . . 259
50.1 Linearization Method . . . 259
50.2 Linearization in Practice . . . 260
50.3 Learning Noisy Parity . . . 261
50.4 Open Problems . . . 262
50.5 Notes and Links . . . 262

**51 Neal Koblitz: Attacks on Cryptosystems** . . . 263
51.1 Early Days of Cryptography . . . 263
51.2 Proving an OS Kernel Is Secure . . . 264
51.3 Provable Security . . . 265
51.4 Provable Security? . . . 266
51.5 Neal's Main Attack . . . 267
51.6 Open Problems . . . 267
51.7 Notes and Links . . . 268

**52 Richard Feynman: Miracle Numbers** . . . 269
52.1 Some Numerology . . . 270
52.2 A Surprising Result . . . 271
52.3 The First-Order Connection . . . 272
52.4 How to Represent the Group . . . 273
52.5 The Proof . . . 273
52.6 Open Problems . . . 274
52.7 Notes and Links . . . 274

**53 Patrick Fischer: Programming Turing Machines** . . . 275
53.1 The Two Theorems . . . 276
53.2 Applications . . . 276
53.3 Proofs of the Theorems . . . 277
53.4 Open Problems . . . 278
53.5 Notes and Links . . . 278

**54 Roger Apéry: Explaining Proofs** . . . 281
54.1 Apéry's Proof . . . 281
54.2 Some Suggestions . . . 282
54.3 Open Problems . . . 285
54.4 Notes and Links . . . 285

**55 Ron Rivest: Mathematical Gifts** . . . 287
55.1 Gift I . . . 287
55.2 Gift II . . . 288
55.3 Gift III . . . 289
55.4 Gift IV . . . 290
55.5 Open Problems . . . 291
55.6 Notes and Links . . . 291

**56 Frank Ryan: The Quarterback Teaches** . . . 293
56.1 Ryan's Seminar . . . 294
56.2 Learning Methods . . . 295
56.3 Open Problems . . . 295
56.4 Notes and Links . . . 295

**57 Leonard Schulman: Associativity** . . . 297
57.1 Multiplication Tables . . . 297
57.2 Testing Associativity . . . 298
57.3 Open Problems . . . 299
57.4 Notes and Links . . . 299

**58 Paul Seymour: Graph Minors** . . . 301
58.1 The Result of Grohe . . . 302
58.2 Fixed-Point Logic with Counting . . . 303
58.3 Why Are Minor Results so Major? . . . 303
58.4 Open Problems . . . 304
58.5 Notes and Links . . . 304

**59 Alfred Tarski: Lower Bounds on Theories** . . . . . 305
59.1 Upper Bounds on the Theory of the Reals . . . . . 305
59.2 Lower Bounds on the Theory of the Reals . . . . . 306
59.3 Lower Bounds on the Complexity of Theories . . . . . 307
59.4 A Recursion Trick . . . . . 307
59.5 A Name Trick . . . . . 308
59.6 Lower Bounds on the Theory of the Complex Numbers? . . . . 308
59.7 Open Problems . . . . . 309
59.8 Notes and Links . . . . . 309

**60 Ken Thompson: Playing Chess** . . . . . 311
60.1 Chess Programs and the Big Match . . . . . 311
60.2 The Book of Chess . . . . . 312
60.3 Building Big Files . . . . . 314
60.4 The Search Problem . . . . . 314
60.5 Shorter Tablebase Descriptions? . . . . . 315
60.6 The Tablebase Graphs . . . . . 316
60.7 The Book as "Deep" Oracle? . . . . . 316
60.8 Open Problems . . . . . 317
60.9 Notes and Links . . . . . 317

**61 Virginia Vassilevska: Fixing Tournaments** . . . . . 319
61.1 Ratings . . . . . 320
61.2 Tournaments . . . . . 320
61.3 Fixing Tournaments . . . . . 321
61.4 Open Problems . . . . . 322
61.5 Notes and Links . . . . . 322

**62 Arkadev Chattopadhyay: Computing Modulo Composites** . . . . . 325
62.1 Representations of Boolean Functions . . . . . 325
62.2 A Question . . . . . 325
62.3 Uniqueness . . . . . 326
62.4 Another Question . . . . . 327
62.5 A Peek Ahead . . . . . 327
62.6 Open Problems . . . . . 328
62.7 Notes and Links . . . . . 328

**63 Charles Bennett: Quantum Protocols** . . . . . 329
63.1 Quantum Protocols . . . . . 330
63.2 Attacks . . . . . 331
63.3 A Theorem . . . . . 332
63.4 Open Problems . . . . . 332
63.5 Notes and Links . . . . . 333