国外数学名著系列
（影印版）3

Yu.I. Manin A. A. Panchishkin

Introduction to Modern Number Theory

Second Edition

现代数论导引

（第二版）

科学出版社
www.sciencep.com

图字:01-2005-6735

Yu. I. Manin, A. A. Panchishkin: Introduction to Modern Number Theory (Second Edition)

图书在版编目(CIP)数据

现代数论导引：第2版＝Introduction to Modern Number Theory(Second Edition)/(俄罗斯)马宁(Manin, Yu. I.)等编著. 影印版. —北京：科学出版社，2006

(国外数学名著系列)

ISBN 7-03-016687-6

Ⅰ. 现…　Ⅱ. 马…　Ⅲ. 数论-英文　Ⅳ. O156

中国版本图书馆CIP数据核字(2005)第154391号

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
中国科学院印刷厂 印刷
科学出版社发行　各地新华书店经销

*

2006年1月第　一　版　　开本：B5(720×1000)
2006年1月第一次印刷　　印张：33 1/2
印数：1—2 500　　　　　字数：630 000

定价：78.00元

(如有印装质量问题，我社负责调换〈科印〉)

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格（Springer）出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了23本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这23本书中，包括基础数学书5本，应用数学书6本与计算数学书12本，其中有些书也具有交叉性质。这些书都是很新的，2000年以后出版的占绝大部分，共计16本，其余的也是1990年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王　元

2005年12月3日

Preface

The present book is a new revised and updated version of "Number Theory I. Introduction to Number Theory" by Yu.I.Manin and A.A.Panchishkin, appeared in 1989 in Moscow (VINITI Publishers) [Ma-PaM], and in English translation [Ma-Pa] of 1995 (Springer Verlag).

The original book had been conceived as a part of a vast project, "Encyclopaedia of Mathematical Sciences". Accordingly, our task was to provide a series of introductory essays to various chapters of number theory, leading the reader from illuminating examples of number theoretic objects and problems, through general notions and theories, developed gradually by many researchers, to some of the highlights of modern mathematics and great, sometimes nebulous designs for future generations.

In preparing this new edition, we tried to keep this initial vision intact. We present many precise definitions, but practically no complete proofs. We try to show the logic of number-theoretic thought and the wide context in which various constructions are made, but for detailed study of the relevant materials the reader will have to turn to original papers or to other monographs. Because of lack of competence and/or space, we had to - reluctantly - omit many fascinating developments.

The new sections written for this edition, include a sketch of Wiles' proof of Fermat's Last Theorem, and relevant techniques coming from a synthesis of various theories of Part II; the whole Part III dedicated to arithmetical cohomology and noncommutative geometry; a report on point counts on varieties with many rational points; the recent polynomial time algorithm for primality testing, and some others subjects.

For more detailed description of the content and suggestions for further reading, see Introduction.

We are very pleased to express our deep gratitude to Prof. M.Marcolli for her essential help in preparing the last part of the new edition. We are very grateful to Prof. H.Cohen for his assistance in updating the book, especially Chapter 2. Many thanks to Prof. Yu.Tschinkel for very useful suggestions, remarks, and updates; he kindly rewrote §5.2 for this edition. We thank Dr.R.Hill and Dr.A.Gewirtz for editing some new sections of this edition, and St.Kühnlein (Universität des Saarlandes) for sending us a detailed list of remarks to the first edition.

Bonn, July 2004

Yu.I.Manin
A.A.Panchishkin

Contents

Part I Problems and Tricks

1 **Elementary Number Theory** ... 9
- 1.1 Problems About Primes. Divisibility and Primality ... 9
  - 1.1.1 Arithmetical Notation ... 9
  - 1.1.2 Primes and composite numbers ... 10
  - 1.1.3 The Factorization Theorem and the Euclidean Algorithm ... 12
  - 1.1.4 Calculations with Residue Classes ... 13
  - 1.1.5 The Quadratic Reciprocity Law and Its Use ... 15
  - 1.1.6 The Distribution of Primes ... 17
- 1.2 Diophantine Equations of Degree One and Two ... 22
  - 1.2.1 The Equation $ax + by = c$ ... 22
  - 1.2.2 Linear Diophantine Systems ... 22
  - 1.2.3 Equations of Degree Two ... 24
  - 1.2.4 The Minkowski–Hasse Principle for Quadratic Forms ... 26
  - 1.2.5 Pell's Equation ... 28
  - 1.2.6 Representation of Integers and Quadratic Forms by Quadratic Forms ... 29
  - 1.2.7 Analytic Methods ... 33
  - 1.2.8 Equivalence of Binary Quadratic Forms ... 35
- 1.3 Cubic Diophantine Equations ... 38
  - 1.3.1 The Problem of the Existence of a Solution ... 38
  - 1.3.2 Addition of Points on a Cubic Curve ... 38
  - 1.3.3 The Structure of the Group of Rational Points of a Non–Singular Cubic Curve ... 40
  - 1.3.4 Cubic Congruences Modulo a Prime ... 47
- 1.4 Approximations and Continued Fractions ... 50
  - 1.4.1 Best Approximations to Irrational Numbers ... 50
  - 1.4.2 Farey Series ... 50
  - 1.4.3 Continued Fractions ... 51

1.4.4 SL_2–Equivalence ... 53
1.4.5 Periodic Continued Fractions and Pell's Equation ... 53
1.5 Diophantine Approximation and the Irrationality ... 55
1.5.1 Ideas in the Proof that $\zeta(3)$ is Irrational ... 55
1.5.2 The Measure of Irrationality of a Number ... 56
1.5.3 The Thue–Siegel–Roth Theorem, Transcendental Numbers, and Diophantine Equations ... 57
1.5.4 Proofs of the Identities (1.5.1) and (1.5.2) ... 58
1.5.5 The Recurrent Sequences a_n and b_n ... 59
1.5.6 Transcendental Numbers and the Seventh Hilbert Problem ... 61
1.5.7 Work of Yu.V. Nesterenko on e^π, [Nes99] ... 61

2 Some Applications of Elementary Number Theory ... 63
2.1 Factorization and Public Key Cryptosystems ... 63
2.1.1 Factorization is Time-Consuming ... 63
2.1.2 One–Way Functions and Public Key Encryption ... 63
2.1.3 A Public Key Cryptosystem ... 64
2.1.4 Statistics and Mass Production of Primes ... 66
2.1.5 Probabilistic Primality Tests ... 66
2.1.6 The Discrete Logarithm Problem and The Diffie-Hellman Key Exchange Protocol ... 67
2.1.7 Computing of the Discrete Logarithm on Elliptic Curves over Finite Fields (ECDLP) ... 68
2.2 Deterministic Primality Tests ... 69
2.2.1 Adleman–Pomerance–Rumely Primality Test: Basic Ideas ... 69
2.2.2 Gauss Sums and Their Use in Primality Testing ... 71
2.2.3 Detailed Description of the Primality Test ... 75
2.2.4 Primes is in P ... 78
2.2.5 The algorithm of M. Agrawal, N. Kayal and N. Saxena . 81
2.2.6 Practical and Theoretical Primality Proving. The ECPP (Elliptic Curve Primality Proving by F.Morain, see [AtMo93b]) ... 81
2.2.7 Primes in Arithmetic Progression ... 82
2.3 Factorization of Large Integers ... 84
2.3.1 Comparative Difficulty of Primality Testing and Factorization ... 84
2.3.2 Factorization and Quadratic Forms ... 84
2.3.3 The Probabilistic Algorithm CLASNO ... 85
2.3.4 The Continued Fractions Method (CFRAC) and Real Quadratic Fields ... 87
2.3.5 The Use of Elliptic Curves ... 90

Part II Ideas and Theories

3 Induction and Recursion 95

3.1 Elementary Number Theory From the Point of View of Logic . 95

3.1.1 Elementary Number Theory 95

3.1.2 Logic 96

3.2 Diophantine Sets 98

3.2.1 Enumerability and Diophantine Sets 98

3.2.2 Diophantineness of enumerable sets 98

3.2.3 First properties of Diophantine sets 98

3.2.4 Diophantineness and Pell's Equation 99

3.2.5 The Graph of the Exponent is Diophantine 100

3.2.6 Diophantineness and Binomial coefficients 100

3.2.7 Binomial coefficients as remainders 101

3.2.8 Diophantineness of the Factorial 101

3.2.9 Factorial and Euclidean Division 101

3.2.10 Supplementary Results 102

3.3 Partially Recursive Functions and Enumerable Sets 103

3.3.1 Partial Functions and Computable Functions 103

3.3.2 The Simple Functions 103

3.3.3 Elementary Operations on Partial functions 103

3.3.4 Partially Recursive Description of a Function 104

3.3.5 Other Recursive Functions 106

3.3.6 Further Properties of Recursive Functions 108

3.3.7 Link with Level Sets 108

3.3.8 Link with Projections of Level Sets 108

3.3.9 Matiyasevich's Theorem 109

3.3.10 The existence of certain bijections 109

3.3.11 Operations on primitively enumerable sets 111

3.3.12 Gödel's function 111

3.3.13 Discussion of the Properties of Enumerable Sets 112

3.4 Diophantineness of a Set and algorithmic Undecidability 113

3.4.1 Algorithmic undecidability and unsolvability 113

3.4.2 Sketch Proof of the Matiyasevich Theorem 113

4 Arithmetic of algebraic numbers 115

4.1 Algebraic Numbers: Their Realizations and Geometry 115

4.1.1 Adjoining Roots of Polynomials 115

4.1.2 Galois Extensions and Frobenius Elements 117

4.1.3 Tensor Products of Fields and Geometric Realizations of Algebraic Numbers 119

4.1.4 Units, the Logarithmic Map, and the Regulator 121

4.1.5 Lattice Points in a Convex Body 123

4.1.6 Deduction of Dirichlet's Theorem From Minkowski's Lemma 125
4.2 Decomposition of Prime Ideals, Dedekind Domains, and Valuations 126
4.2.1 Prime Ideals and the Unique Factorization Property . . . 126
4.2.2 Finiteness of the Class Number 128
4.2.3 Decomposition of Prime Ideals in Extensions 129
4.2.4 Decomposition of primes in cyslotomic fields 131
4.2.5 Prime Ideals, Valuations and Absolute Values 132
4,3 Local and Global Methods 134
4.3.1 p–adic Numbers 134
4.3.2 Applications of p–adic Numbers to Solving Congruences 138
4.3.3 The Hilbert Symbol 139
4.3.4 Algebraic Extensions of $\mathbb{Q}_p$, and the Tate Field 142
4.3.5 Normalized Absolute Values 143
4.3.6 Places of Number Fields and the Product Formula 145
4.3.7 Adeles and Ideles 146
The Ring of Adeles. 146
The Idele Group 149
4.3.8 The Geometry of Adeles and Ideles 149
4.4 Class Field Theory 155
4.4.1 Abelian Extensions of the Field of Rational Numbers . . 155
4.4.2 Frobenius Automorphisms of Number Fields and Artin's Reciprocity Map 157
4.4.3 The Chebotarev Density Theorem 159
4.4.4 The Decomposition Law and the Artin Reciprocity Map 159
4.4.5 The Kernel of the Reciprocity Map 160
4.4.6 The Artin Symbol 161
4.4.7 Global Properties of the Artin Symbol 162
4.4.8 A Link Between the Artin Symbol and Local Symbols . . 163
4.4.9 Properties of the Local Symbol 164
4.4.10 An Explicit Construction of Abelian Extensions of a Local Field, and a Calculation of the Local Symbol 165
4.4.11 Abelian Extensions of Number Fields 168
4.5 Galois Group in Arithetical Problems 172
4.5.1 Dividing a circle into n equal parts 172
4.5.2 Kummer Extensions and the Power Residue Symbol . . . 175
4.5.3 Galois Cohomology 178
4.5.4 A Cohomological Definition of the Local Symbol 182
4.5.5 The Brauer Group, the Reciprocity Law and the Minkowski–Hasse Principle 184

5 Arithmetic of algebraic varieties 191
5.1 Arithmetic Varieties and Basic Notions of Algebraic Geometry 191
5.1.1 Equations and Rings 191
5.1.2 The set of solutions of a system 191
5.1.3 Example: The Language of Congruences 192
5.1.4 Equivalence of Systems of Equations 192
5.1.5 Solutions as K-algebra Homomorphisms 192
5.1.6 The Spectrum of A Ring 193
5.1.7 Regular Functions 193
5.1.8 A Topology on Spec(A) 193
5.1.9 Schemes 196
5.1.10 Ring-Valued Points of Schemes 197
5.1.11 Solutions to Equations and Points of Schemes 198
5.1.12 Chevalley's Theorem 199
5.1.13 Some Geometric Notions 199
5.2 Geometric Notions in the Study of Diophantine equations 202
5.2.1 Basic Questions 202
5.2.2 Geometric classification 203
5.2.3 Existence of Rational Points and Obstructions to the Hasse Principle 204
5.2.4 Finite and Infinite Sets of Solutions 206
5.2.5 Number of points of bounded height 208
5.2.6 Height and Arakelov Geometry 211
5.3 Elliptic curves, Abelian Varieties, and Linear Groups 213
5.3.1 Algebraic Curves and Riemann Surfaces 213
5.3.2 Elliptic Curves 213
5.3.3 Tate Curve and Its Points of Finite Order 219
5.3.4 The Mordell – Weil Theorem and Galois Cohomology . . 221
5.3.5 Abelian Varieties and Jacobians 226
5.3.6 The Jacobian of an Algebraic Curve 228
5.3.7 Siegel's Formula and Tamagawa` Measure 231
5.4 Diophantine Equations and Galois Representations 238
5.4.1 The Tate Module of an Elliptic Curve 238
5.4.2 The Theory of Complex Multiplication 240
5.4.3 Characters of l-adic Representations 242
5.4.4 Representations in Positive Characteristic 243
5.4.5 The Tate Module of a Number Field 244
5.5 The Theorem of Faltings and Finiteness Problems in Diophantine Geometry 247
5.5.1 Reduction of the Mordell Conjecture to the finiteness Conjecture 247
5.5.2 The Theorem of Shafarevich on Finiteness for Elliptic Curves 249
5.5.3 Passage to Abelian varieties 250
5.5.4 Finiteness problems and Tate's conjecture 252

5.5.5 Reduction of the conjectures of Tate to the finiteness properties for isogenies . . . 253
5.5.6 The Faltings–Arakelov Height . . . 255
5.5.7 Heights under isogenies and Conjecture T . . . 257

6 Zeta Functions and Modular Forms . . . 261
6.1 Zeta Functions of Arithmetic Schemes . . . 261
6.1.1 Zeta Functions of Arithmetic Schemes . . . 261
6.1.2 Analytic Continuation of the Zeta Functions . . . 263
6.1.3 Schemes over Finite Fields and Deligne's Theorem . . . 263
6.1.4 Zeta Functions and Exponential Sums . . . 267
6.2 L-Functions, the Theory of Tate and Explicite Formulae . . . 272
6.2.1 L-Functions of Rational Galois Representations . . . 272
6.2.2 The Formalism of Artin . . . 274
6.2.3 Example: The Dedekind Zeta Function . . . 276
6.2.4 Hecke Characters and the Theory of Tate . . . 278
6.2.5 Explicit Formulae . . . 285
6.2.6 The Weil Group and its Representations . . . 288
6.2.7 Zeta Functions, L-Functions and Motives . . . 290
6.3 Modular Forms and Euler Products . . . 296
6.3.1 A Link Between Algebraic Varieties and L–Functions . . 296
6.3.2 Classical modular forms . . . 296
6.3.3 Application: Tate Curve and Semistable Elliptic Curves 299
6.3.4 Analytic families of elliptic curves and congruence subgroups . . . 301
6.3.5 Modular forms for congruence subgroups . . . 302
6.3.6 Hecke Theory . . . 304
6.3.7 Primitive Forms . . . 310
6.3.8 Weil's Inverse Theorem . . . 312
6.4 Modular Forms and Galois Representations . . . 317
6.4.1 Ramanujan's congruence and Galois Representations . . . 317
6.4.2 A Link with Eichler–Shimura's Construction . . . 319
6.4.3 The Shimura–Taniyama–Weil Conjecture . . . 320
6.4.4 The Conjecture of Birch and Swinnerton–Dyer . . . 321
6.4.5 The Artin Conjecture and Cusp Forms . . . 327
The Artin conductor . . . 329
6.4.6 Modular Representations over Finite Fields . . . 330
6.5 Automorphic Forms and The Langlands Program . . . 332
6.5.1 A Relation Between Classical Modular Forms and Representation Theory . . . 332
6.5.2 Automorphic L-Functions . . . 335
Further analytic properties of automorphic L-functions . 338
6.5.3 The Langlands Functoriality Principle . . . 338
6.5.4 Automorphic Forms and Langlands Conjectures . . . 339

7 Fermat's Last Theorem and Families of Modular Forms 341

7.1 Shimura–Taniyama–Weil Conjecture and Reciprocity Laws 341

7.1.1 Problem of Pierre de Fermat (1601–1665) 341

7.1.2 G.Lamé's Mistake 342

7.1.3 A short overview of Wiles' Marvelous Proof 343

7.1.4 The STW Conjecture 344

7.1.5 A connection with the Quadratic Reciprocity Law 345

7.1.6 A complete proof of the STW conjecture 345

7.1.7 Modularity of semistable elliptic curves 348

7.1.8 Structure of the proof of theorem 7.13 (Semistable STW Conjecture) 349

7.2 Theorem of Langlands-Tunnell and Modularity Modulo 3 352

7.2.1 Galois representations: preparation 352

7.2.2 Modularity modulo p 354

7.2.3 Passage from cusp forms of weight one to cusp forms of weight two 355

7.2.4 Preliminary review of the stages of the proof of Theorem 7.13 on modularity 356

7.3 Modularity of Galois representations and Universal Deformation Rings 357

7.3.1 Galois Representations over local Noetherian algebras 357

7.3.2 Deformations of Galois Representations 357

7.3.3 Modular Galois representations 359

7.3.4 Admissible Deformations and Modular Deformations 361

7.3.5 Universal Deformation Rings 363

7.4 Wiles' Main Theorem and Isomorphism Criteria for Local Rings 365

7.4.1 Strategy of the proof of the Main Theorem 7.33 365

7.4.2 Surjectivity of φ_Σ 365

7.4.3 Constructions of the universal deformation ring R_Σ 367

7.4.4 A sketch of a construction of the universal modular deformation ring $\mathbb{T}_\Sigma$ 368

7.4.5 Universality and the Chebotarev density theorem 369

7.4.6 Isomorphism Criteria for local rings 370

7.4.7 J-structures and the second criterion of isomorphism of local rings 371

7.5 Wiles' Induction Step: Application of the Criteria and Galois Cohomology 373

7.5.1 Wiles' induction step in the proof of Main Theorem 7.33 373

7.5.2 A formula relating $\#\Phi_{R_\Sigma}$ and $\#\Phi_{R_{\Sigma'}}$: preparation 374

7.5.3 The Selmer group and Φ_{R_Σ} 375

7.5.4 Infinitesimal deformations 375

7.5.5 Deformations of type $\mathcal{D}_\Sigma$ 377

7.6 The Relative Invariant, the Main Inequality and The Minimal Case . . . 382
7.6.1 The Relative invariant . . . 382
7.6.2 The Main Inequality . . . 383
7.6.3 The Minimal Case . . . 386
7.7 End of Wiles' Proof and Theorem on Absolute Irreducibility . . 388
7.7.1 Theorem on Absolute Irreducibility . . . 388
7.7.2 From $p = 3$ to $p = 5$ . . . 390
7.7.3 Families of elliptic curves with fixed $\overline{\rho}_{5,E}$ . . . 391
7.7.4 The end of the proof . . . 392
The most important insights. . . . 393

Part III Analogies and Visions

III-0 Introductory survey to part III: motivations and description . . . 397
III.1 Analogies and differences between numbers and functions: ∞-point, Archimedean properties etc. . . . 397
III.1.1 Cauchy residue formula and the product formula . . . 397
III.1.2 Arithmetic varieties. . . . 398
III.1.3 Infinitesimal neighborhoods of fibers . . . 398
III.2 Arakelov geometry, fiber over ∞, cycles, Green functions (d'après Gillet-Soulé) . . . 399
III.2.1 Arithmetic Chow groups . . . 400
III.2.2 Arithmetic intersection theory and arithmetic Riemann-Roch theorem . . . 401
III.2.3 Geometric description of the closed fibers at infinity . . . 402
III.3 ζ-functions, local factors at ∞, Serre's Γ-factors . . . 404
III.3.1 Archimedean L-factors . . . 405
III.3.2 Deninger's formulae . . . 406
III.4 A guess that the missing geometric objects are noncommutative spaces . . . 407
III.4.1 Types and examples of noncommutative spaces, and how to work with them. Noncommutative geometry and arithmetic . . . 407
Isomorphism of noncommutative spaces and Morita equivalence . . . 409
The tools of noncommutative geometry . . . 410
III.4.2 Generalities on spectral triples . . . 411
III.4.3 Contents of Part III: description of parts of this program412

8 Arakelov Geometry and Noncommutative Geometry 415
8.1 Schottky Uniformization and Arakelov Geometry 415
8.1.1 Motivations and the context of the work of Consani-Marcolli 415
8.1.2 Analytic construction of degenerating curves over complete local fields 416
8.1.3 Schottky groups and new perspectives in Arakelov geometry 420
Schottky uniformization and Schottky groups 421
Fuchsian and Schottky uniformization. 424
8.1.4 Hyperbolic handlebodies 425
Geodesics in $\mathfrak{X}_\Gamma$ 427
8.1.5 Arakelov geometry and hyperbolic geometry 427
Arakelov Green function 427
Cross ratio and geodesics 428
Differentials and Schottky uniformization 428
Green function and geodesics 430
8.2 Cohomological Constructions 431
8.2.1 Archimedean cohomology 431
Operators 433
SL(2, $\mathbb{R}$) representations 434
8.2.2 Local factor and Archimedean cohomology 435
8.2.3 Cohomological constructions 436
8.2.4 Zeta function of the special fiber and Reidemeister torsion 437
8.3 Spectral Triples, Dynamics and Zeta Functions 440
8.3.1 A dynamical theory at infinity 442
8.3.2 Homotopy quotion 443
8.3.3 Filtration 444
8.3.4 Hilbert space and grading 446
8.3.5 Cuntz–Krieger algebra 446
Spectral triples for Schottky groups 448
8.3.6 Arithmetic surfaces: homology and cohomology 449
8.3.7 Archimedean factors from dynamics 450
8.3.8 A Dynamical theory for Mumford curves 450
Genus two example 452
8.3.9 Cohomology of $\mathcal{W}(\Delta/\Gamma)_T$ 454
8.3.10 Spectral triples and Mumford curves 456
8.4 Reduction mod ∞ 458
8.4.1 Homotopy quotients and "reduction mod infinity" 458
8.4.2 Baum-Connes map 460

References 461

Index 503

Introduction

Among the various branches of mathematics, number theory is characterized to a lesser degree by its primary subject ("integers") than by a psychological attitude. Actually, number theory also deals with rational, algebraic, and transcendental numbers, with some very specific analytic functions (such as *Dirichlet series* and *modular forms*), and with some geometric objects (such as *lattices* and *schemes over* $\mathbb{Z}$). The question whether a given article belongs to number theory is answered by its author's system of values. If arithmetic is not there, the paper will hardly be considered as number–theoretical, even if it deals exclusively with integers and congruences. On the other hand, any mathematical tool, say, homotopy theory or dynamical systems may become an important source of number–theoretical inspiration. For this reason, combinatorics and the theory of recursive functions are not usually associated with number theory, whereas modular functions are.

In this book we interpret number theory broadly. There are compelling reasons to adopt this viewpoint.

First of all, the integers constitute (together with geometric images) one of the primary subjects of mathematics in general. Because of this, the history of elementary number theory is as long as the history of all mathematics, and the history of modern mathematic began when "numbers" and "figures" were united by the concept of coordinates (which in the opinion of I.R.Shafarevich also forms the basic idea of algebra, see [Sha87]).

Moreover, integers constitute the basic universe of discrete symbols and therefore a universe of all logical constructions conceived as symbolic games. Of course, as an act of individual creativity, mathematics does not reduce to logic. Nevertheless, in the collective consciousness of our epoch there does exist an image of mathematics as a potentially complete, immense and precise logical construction. While the unrealistic rigidity of this image is well understood, there is still a strong tendency to keep it alive. The last but not the least reason for this is the computer reality of our time, with its very strict demands on the logical structure of a particular kind of mathematical production: software.

It was a discovery of our century, due to Hilbert and Gödel above all, that the properties of integers are general properties of discrete systems and therefore properties of the world of mathematical reasoning. We understand now that this idea can be stated as a theorem that provability in an arbitrary finitistic formal system is equivalent to a statement about decidability of a system of Diophantine equations (cf. below). This paradoxical fact shows that number theory, being a small part of mathematical knowledge, potentially embraces all this knowledge. If Gauss' famous motto on arithmetic [*] needs justification, this theorem can be considered as such.

We had no intention of presenting in this report the whole of number theory. That would be impossible anyway. Therefore, we had to consider the usual choice and organization problems. Following some fairly traditional classification principles, we could have divided the bulk of this book into the following parts:

1. Elementary number theory.
2. Arithmetic of algebraic numbers.
3. Number-theoretical structure of the continuum (approximation theory, transcendental numbers, geometry of numbers Minkowski style, metric number theory etc.).
4. Analytic number theory (circle method, exponential sums, Dirichlet series and explicit formulae, modular forms).
5. Algebraic-geometric methods in the theory of Diophantine equations.
6. Miscellany ("wastebasket").

We preferred, however, a different system, and decided to organize our subject into three large subheadings which shall be described below. Because of our incompetence and/or lack of space we then had to omit many important themes that were initially included into our plan. We shall nevertheless briefly explain its concepts in order to present in a due perspective both this book and subsequent number-theoretical issues of this series.

Part I. *Problems and Tricks*

The choice of the material for this part was guided by the following principles.

In number theory, like in no other branch of mathematics, a bright young person with a minimal mathematical education can sometimes work wonders using inventive tricks. There are a lot of unsolved elementary problems waiting

[*] "... Mathematik ist die Königin von Wissenschaften und Arithmetik die Königin von Mathematik. ... in allen Relationen sie wird zum ersten Rank erlaubt." -Gauss. ..., cf. e.g. `http://www.geocities.com/RainForest/Vines/2977/gauss/deutsch/quotes.html` ("Mathematics is the queen of sciences and arithmetic the queen of mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations she is entitled to the first rank." -Gauss. Sartorius von Walterhausen: Gauss zum Gedächtniss. (Leipzig, 1856), p.79.)