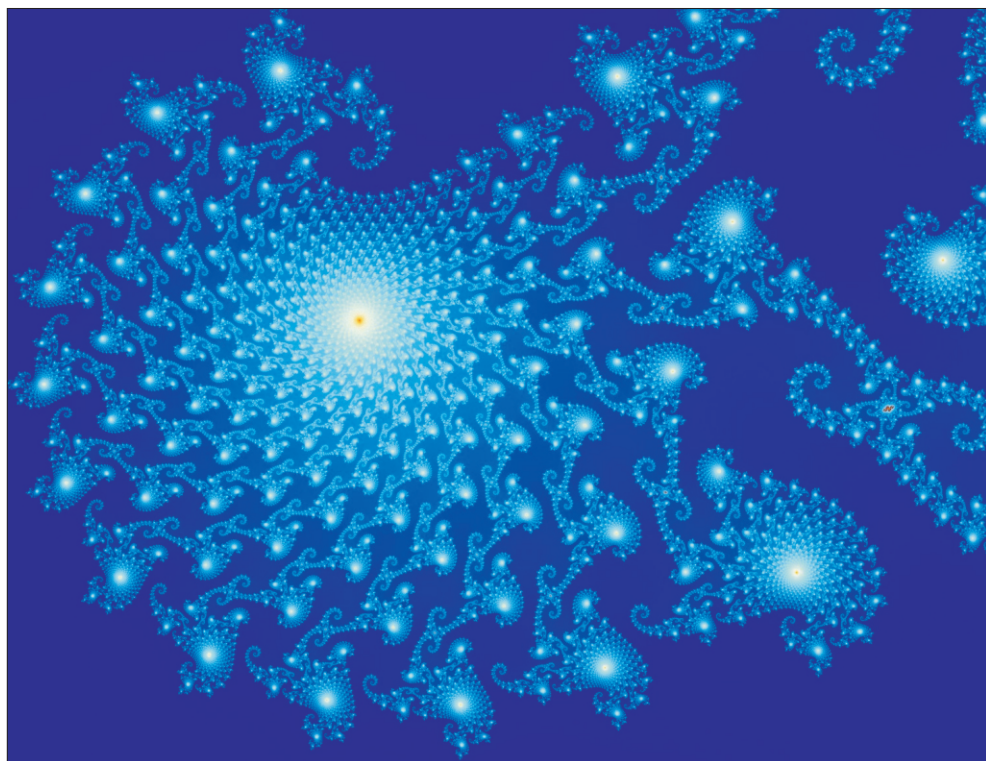


Number Theory and Algebraic Equations

Odile Marie-Thérèse Pons



Number Theory and Algebraic Equations

Odile Marie-Thérèse Pons



Published by
Science Publishing Group
548 Fashion Avenue
New York, NY 10018, U.S.A.
<http://www.sciencepublishinggroup.com>

ISBN: 978-1-940366-74-6



© Odile Marie-Thérèse Pons 2016

The book is published with partial-open access by Science Publishing Group and distributed under the terms of the Creative Commons Attribution 3.0 Unported License (<http://creativecommons.org/licenses/by/3.0/>) which permits any use, distribution, and reproduction in any medium, provided that the original author(s) and source are properly credited.

Preface

The factorization of every integer as a product of its prime divisors is the basis of the arithmetics and the search of rules to compute them for large numbers is the origin of the elementary number theory, it is related to the factorization of polynomials. Fermat's theorems and his comments on the Diophantine equations are well-known mathematical texts of the XVII-th century, they are connections between arithmetics and geometry through equations for the intersections of elliptic curves or geometric solids. They are generally studied separately in algebra and analysis. Most proofs of the number theory rely on field properties and Galois theory, their applications to the geometry send them back to their origin.

Many early publications have stated properties of numbers without proofs and the attempts to solve them remained unsuccessful for a long time. Fermat's last theorem concerning the non existence of non zero integer solutions of the equations

$$x^n + y^n = z^n$$

was unsolved until recently, partial proofs suppose the knowledge of the existence of roots of homogeneous polynomials of degree n but the premisses have not been asserted. The extension of theorems with primes to composite numbers is often difficult and intricate, many questions are not closed.

The conjectures of the separation of integers, polynomials or curves as sums or products of elements belonging to specific families are still open challenges though they may be computationally validated on large scales in the related fields. The main results of this domain have been proved during the XVIII-th century by Euler, Lagrange, Legendre, Gauss, Dirichlet and others with the development of the modern algebra. After the publication of tables of prime number during the previous century, they published tables of prime polynomials.

Riemann's hypothesis about the complex zeros of Euler's function ζ is another conjecture, it is connected to the evaluation of the number $\pi(x)$ of primes until x and to expansions of the functions $\pi(x)$ and $\zeta(x)$.

The book is an undergraduate and graduate course for students in mathematics, the concepts are illustrated by many formal and numerical examples. It covers the classical number theory and new generalizations are introduced. My proofs are often simpler than the classical ones, they include an elementary proof of Fermat's last theorem and extensions. Chapter 1 introduces the reader to the representation and the classification of the numbers. Chapter 2 focuses on Fermat's first theorem, its extensions and applications to the quadratic residues and the representation of integers as sums of squares. Chapter 3 develops solutions of Diophantine equations and algebraic equations, I prove Fermat's last theorem, Catalan's conjecture and study equations that extend Fermat's theorem such as Dirichlet's equations for $x^5 + y^5$. Chapter 4 deals with the distributions of the prime integers and the factorization of integer polynomials, Chapter 2-4 are much indebted to Legendre writings. The functions Gamma and zeta and other series are related to the cardinal of the primes, Chapter 5 recalls their properties with detailed proofs of their expansions. Chapter 6 focuses on the algebraic number theory in fields of decomposition of irreducible polynomials and Galois's groups. Chapter 7 applies the field theory to polynomials and functional problems, throughout examples illustrate the theory.

Odile M.-T. Pons

July 2016

Contents

1	Introduction	1
1.1	Factorization of the Integers	4
1.2	Polygonal Numbers	13
1.3	Quadratic Fields	21
1.4	Quadratic Equations	26
1.5	Exercises	30
2	Fermat's First Theorem and Quadratic Residues	31
2.1	Fermat's First Theorem	33
2.2	Divisors of an Integer	36
2.3	Quadratic Residues	38
2.4	Wilson's Theorem and Sums of Squares	49
2.5	Euler's $\phi(n)$	55
2.6	Exercises	56

3	Algebraic Equations and Fermat's Last Theorem	57
3.1	Algebraic Equations	59
3.2	Fermat's Last Theorem	69
3.3	Catalan's Equation	74
3.4	Generalizations of Fermat's Last Theorem	77
3.5	Exercises	84
4	Prime Numbers and Irrational Numbers	85
4.1	Cardinal of the Primes in Intervals	87
4.2	Legendre's Quadratic Equations	91
4.3	Complex Quadratic Rings	102
4.4	Algebraic Numbers of Degree n	104
4.5	Equations with Several Variables	109
4.6	Twin-primes	114
4.7	Exercises	116
5	Euler's Functions	117
5.1	Definition	119
5.2	Approximations of the Function $\pi(x)$	123
5.3	Approximations of the Function Gamma	125
5.4	Riemann's Equations for ζ_s	130
5.5	The Alternating Series	133

5.6	Bernoulli Polynomials	137
5.7	Trigonometric Expansions	142
5.8	The Hurwitz Zeta Function	144
5.9	Logarithm of ζ_s	151
5.10	Exercises	152
6	Automorphisms	153
6.1	Rings	155
6.2	Algebraic Extension of a Field	161
6.3	Galois's Extension	170
6.4	Galois's Theory	174
6.5	Equation Solvable by Radicals	177
6.6	Exercises	186
7	Functional Equations	187
7.1	Fermat's First Theorem for Polynomials	189
7.2	Polynomials in F_p	194
7.3	Quadratic Equations for Polynomials	198
7.4	Complex Algebraic Fields	206
7.5	Exercises	209
8	Exercises	211
8.1	Introduction	213

Contents

8.2 Fermat’s First Theorem and Quadratic Residues 214

8.3 Algebraic Equations and Fermat’s Last Theorem 215

8.4 Prime Numbers and Irrational Numbers 217

8.5 The Function Zeta 219

8.6 Automorphisms 223

8.7 Functional Equations 225