

Invitation to the Mathematics of Fermat–Wiles

Yves Hellegouarch

University of Caen, France

This work has been published with the help of
the French Ministère de la Culture – Centre national du livre



ACADEMIC PRESS

An imprint of Elsevier

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

CONTENTS

Foreword	viii
1 Paths	1
1.1 Diophantus and his <i>Arithmetica</i>	2
1.2 Translations of Diophantus	2
1.3 Fermat	3
1.4 Infinite descent	4
1.5 Fermat's "theorem" in degree 4	7
1.6 The theorem of two squares	9
1.6.1 A modern proof	10
1.6.2 "Fermat-style" proof of the crucial theorem	12
1.6.3 Representations as sums of two squares	13
1.7 Euler-style proof of Fermat's last theorem for $n = 3$	16
1.8 Kummer, 1847	18
1.8.1 The ring of integers of $\mathbb{Q}(\zeta)$	18
1.8.2 A lemma of Kummer on the units of $\mathbb{Z}[\zeta]$	23
1.8.3 The ideals of $\mathbb{Z}[\zeta]$	25
1.8.4 Kummer's proof (1847)	26
1.8.5 Regular primes	31
1.9 The current approach	33
Exercises and problems	35
2 Elliptic functions	68
2.1 Elliptic integrals	68
2.2 The discovery of elliptic functions in 1718	71
2.3 Euler's contribution (1753)	75
2.4 Elliptic functions: structure theorems	77
2.5 Weierstrass-style elliptic functions	80
2.6 Eisenstein series	85
2.7 The Weierstrass cubic	87
2.8 Abel's theorem	89

2.9	Loxodromic functions	92
2.10	The function ρ	95
2.11	Computation of the discriminant	97
2.12	Relation to elliptic functions	99
	Exercises and problems	101
3	Numbers and groups	118
3.1	Absolute values on $\mathbb{Q}$	118
3.2	Completion of a field equipped with an absolute value	123
3.3	The field of p -adic numbers	127
3.4	Algebraic closure of a field	131
3.5	Generalities on the linear representations of groups	134
3.6	Galois extensions	140
3.6.1	The Galois correspondence	141
3.6.2	Questions of dimension	143
3.6.3	Stability	146
3.6.4	Conclusions	146
3.7	Resolution of algebraic equations	149
3.7.1	Some general principles	149
3.7.2	Resolution of the equation of degree three	152
	Exercises and problems	155
4	Elliptic curves	172
4.1	Cubics and elliptic curves	172
4.2	Bézout's theorem	179
4.3	Nine-point theorem	183
4.4	Group laws on an elliptic curve	185
4.5	Reduction modulo p	189
4.6	N -division points of an elliptic curve	192
4.6.1	2-division points	192
4.6.2	3-division points	193
4.6.3	n -division points of an elliptic curve defined over $\mathbb{Q}$	194
4.7	A most interesting Galois representation	195
4.8	Ring of endomorphisms of an elliptic curve	197
4.9	Elliptic curves over a finite field	202
4.10	Torsion on an elliptic curve defined over $\mathbb{Q}$	205
4.11	Mordell–Weil theorem	211
4.12	Back to the definition of elliptic curves	211
4.13	Formulae	215
4.14	Minimal Weierstrass equations (over $\mathbb{Z}$)	218
4.15	Hasse–Weil L -functions	223
4.15.1	Riemann zeta function	223
4.15.2	Artin zeta function	224
4.15.3	Hasse–Weil L -function	226
	Exercises and problems	228

5	Modular forms	255
5.1	Brief historical overview	255
5.2	The theta functions	260
5.3	Modular forms for the modular group $SL_2(\mathbb{Z})/\{I, -I\}$	274
5.3.1	Modular properties of the Eisenstein series	274
5.3.2	The modular group	280
5.3.3	Definition of modular forms and functions	287
5.4	The space of modular forms of weight k for $SL_2(\mathbb{Z})$	289
5.5	The fifth operation of arithmetic	294
5.6	The Petersson Hermitian product	297
5.7	Hecke forms	299
5.7.1	Hecke operators for $SL_2(\mathbb{Z})$	300
5.8	Hecke's theory	304
5.8.1	The Mellin transform	306
5.8.2	Functional equations for the functions $L(f, s)$	307
5.9	Wiles' theorem	308
	Exercises and problems	313
6	New paradigms, new enigmas	325
6.1	A second definition of the ring $\mathbb{Z}_p$ of p -adic integers	326
6.2	The Tate module $T_\ell(E)$	328
6.3	A marvellous result	330
6.4	Tate loxodromic functions	331
6.5	Curves $E_{A,B,C}$	332
6.5.1	Reduction of certain curves $E_{A,B,C}$	333
6.5.2	Property of the field K_p associated to E_{a^p, b^p, c^p}	335
6.5.3	Summary of the properties of E_{a^p, b^p, c^p}	335
6.6	The Serre conjectures	336
6.7	Mazur–Ribet's theorem	339
6.7.1	Mazur–Ribet's theorem	340
6.7.2	Other applications	341
6.8	Szpiro's conjecture and the abc conjecture	343
6.8.1	Szpiro's conjecture	343
6.8.2	abc conjecture	344
6.8.3	Consequences	344
	Exercises and problems	348
	Appendix: The origin of the elliptic approach to Fermat's last theorem	359
	Bibliography	371
	Index	375