Pure and Applied Mathematics:
A Wiley Series of Texts, Monographs, and Tracts

SECOND EDITION

Primes of the Form $x^2 + ny^2$

Fermat, Class Field Theory, and Complex Multiplication

$$p \neq 5 \text{ prime}$$
$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20$$

$$L = \text{Hilbert class field of } K$$
$$C(\mathcal{O}_K) \simeq \text{Gal}(L/K)$$

David A. Cox

$$j(\sqrt{-14}) =$$
$$2^3\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right)^3$$

WILEY

PRIMES OF THE FORM $x^2 + ny^2$

PURE AND APPLIED MATHEMATICS

A Wiley Series of Texts, Monographs, and Tracts

Founded by RICHARD COURANT
Editors Emeriti: MYRON B. ALLEN III, DAVID A. COX, PETER HILTON, HARRY HOCHSTADT, PETER LAX, JOHN TOLAND

A complete list of the titles in this series appears at the end of this volume.

PRIMES OF THE FORM $x^2 + ny^2$

Fermat, Class Field Theory, and Complex Multiplication

Second Edition

DAVID A. COX
Department of Mathematics
Amherst College
Amherst, Massachusetts

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Cox, David A.
Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication /
David A. Cox. — Second edition.
pages cm
Originally published: Primes of the form $x^2 + ny^2$, 1989.
Includes bibliographical references and index.
ISBN 978-1-118-39018-4 (cloth)
1. Numbers, Prime. 2. Mathematics. I. Title. II. Title: Primes of the form $x^2 + ny^2$.
QA246.C69 2013
512.7'23—dc23 2013000406

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE TO THE FIRST EDITION ix

PREFACE TO THE SECOND EDITION xi

NOTATION xiii

INTRODUCTION 1

CHAPTER ONE: FROM FERMAT TO GAUSS

§1. FERMAT, EULER AND OUADRATIC RECIPROCITY 7

A. Fermat 8
B. Euler 9
C. $p = x^2 + ny^2$ and Quadratic Reciprocity 11
D. Beyond Quadratic Reciprocity 17
E. Exercises 19

§2. LAGRANGE, LEGENDRE AND QUADRATIC FORMS 22

A. Quadratic Forms 22

B. $p = x^2 + ny^2$ and Quadratic Forms 27
C. Elementary Genus Theory 30
D. Lagrange and Legendre 34
E. Exercises 39

§3. GAUSS, COMPOSITION AND GENERA 42

A. Composition and the Class Group 43
B. Genus Theory 48
C. $p = x^2 + ny^2$ and Euler's Convenient Numbers 53
D. Disquisitiones Arithmeticae 57
E. Exercises 59

§4. CUBIC AND BIQUADRATIC RECIPROCITY 67

A. $\mathbb{Z}[\omega]$ and Cubic Reciprocity 67
B. $\mathbb{Z}[i]$ and Biquadratic Reciprocity 73
C. Gauss and Higher Reciprocity 75
D. Exercises 80

CHAPTER TWO: CLASS FIELD THEORY

§5. THE HILBERT CLASS FIELD AND $p = x^2 + ny^2$ 87

A. Number Fields 88
B. Quadratic Fields 92
C. The Hilbert Class Field 94
D. Solution of $p = x^2 + ny^2$ for Infinitely Many n 98
E. Exercises 103

§6. THE HILBERT CLASS FIELD AND GENUS THEORY 108

A. Genus Theory for Field Discriminants 109
B. Applications to the Hilbert Class Field 114
C. Exercises 116

§7. ORDERS IN IMAGINARY QUADRATIC FIELDS 120

A. Orders in Quadratic Fields 120
B. Orders and Quadratic Forms 123
C. Ideals Prime to the Conductor 129
D. The Class Number 132
E. Exercises 136

§8. CLASS FIELD THEORY AND THE ČEBOTAREV DENSITY THEOREM 144

A. The Theorems of Class Field Theory 144

B. The Čebotarev Density Theorem 152
C. Norms and Ideles 156
D. Exercises 157

§9. RING CLASS FIELDS AND $p = x^2 + ny^2$ 162

A. Solution of $p = x^2 + ny^2$ for All n 162
B. The Ring Class Fields of $\mathbb{Z}[\sqrt{-27}]$ and $\mathbb{Z}[\sqrt{-64}]$ 166
C. Primes Represented by Positive Definite Quadratic Forms 170
D. Ring Class Fields and Generalized Dihedral Extensions 172
E. Exercises 174

CHAPTER THREE: COMPLEX MULTIPLICATION

§10. ELLIPTIC FUNCTIONS AND COMPLEX MULTIPLICATION 181

A. Elliptic Functions and the Weierstrass $\wp$-Function 182
B. The j-Invariant of a Lattice 187
C. Complex Multiplication 190
D. Exercises 197

§11. MODULAR FUNCTIONS AND RING CLASS FIELDS 200

A. The j-Function 200
B. Modular Functions for $\Gamma_0(m)$ 205
C. The Modular Equation $\Phi_m(X, Y)$ 210
D. Complex Multiplication and Ring Class Fields 214
E. Exercises 220

§12. MODULAR FUNCTIONS AND SINGULAR j-INVARIANTS 226

A. The Cube Root of the j-Function 226
B. The Weber Functions 232
C. j-Invariants of Orders of Class Number 1 237
D. Weber's Computation of $j(\sqrt{-14})$ 239
E. Imaginary Quadratic Fields of Class Number 1 247
F. Exercises 250

§13. THE CLASS EQUATION 261

A. Computing the Class Equation 262
B. Computing the Modular Equation 268
C. Theorems of Deuring, Gross and Zagier 272
D. Exercises 277

CHAPTER FOUR: ADDITIONAL TOPICS

§14. ELLIPTIC CURVES 283

A. Elliptic Curves and Weierstrass Equations 284
B. Complex Multiplication and Elliptic Curves 287
C. Elliptic Curves over Finite Fields 290
D. Elliptic Curve Primality Tests 297
E. Exercises 304

§15. SHIMURA RECIPROCITY 309

A. Modular Functions and Shimura Reciprocity 309
B. Extended Ring Class Fields 313
C. Shimura Reciprocity for Extended Ring Class Fields 315
D. Shimura Reciprocity for Ring Class Fields 318
E. The Idelic Approach 324
F. Exercises 328

REFERENCES **335**

ADDITIONAL REFERENCES **343**

A. References Added to the Text 343
B. Further Reading for Chapter One 345
C. Further Reading for Chapter Two 345
D. Further Reading for Chapter Three 345
E. Further Reading for Chapter Four 346

INDEX **347**

PREFACE TO THE FIRST EDITION

Several years ago, while reading Weil's *Number Theory: An Approach Through History*, I noticed a conjecture of Euler concerning primes of the form $x^2 + 14y^2$. That same week I picked up Cohn's A *Classical Invitation to Algebraic Numbers and Class Fields* and saw the same example treated from the point of view of the Hilbert class field. The coincidence made it clear that something interesting was going on, and this book is my attempt to tell the story of this wonderful part of mathematics.

I am an algebraic geometer by training, and number theory has always been more of an avocation than a profession for me. This will help explain some of the curious omissions in the book. There may also be errors of history or attribution (for which I take full responsibility), and doubtless some of the proofs can be improved. Corrections and comments are welcome!

I would like to thank my colleagues in the number theory seminars of Oklahoma State University and the Five Colleges (Amherst College, Hampshire College, Mount Holyoke College, Smith College and the University of Massachusetts) for the opportunity to present material from this book in preliminary form. Special thanks go to Dan Flath and Peter Norman for their comments on earlier versions of the manuscript. I also thank the reference librarians at Amherst College and Oklahoma Slate University for their help in obtaining books through interlibrary loan.

DAVID A. COX

Amherst, Massachsusetts
August 1989

PREFACE TO THE SECOND EDITION

The philosophy of the second edition is to preserve as much of the original text as possible. The major changes are:

- A new §15 on Shimura reciprocity has been added, based on work of Peter Stevenhagen and Alice Gee [A10, A11, A23] and Bumkyo Cho [A6].
- The fifteen sections are now organized into four chapters:
  - The original §§1–13, which present a complete solution of $p = x^2 + ny^2$, now constitute Chapters One, Two and Three.
  - The new Chapter Four consists of the original §14 (on elliptic curves) and the new §15 (on Shimura reciprocity).
- An "Additional References" section has been added to supplement the original references [1]–[112]. This section is divided into five parts:
  - The first part consists of references [A1]–[A24] that are cited in the text. These references (by no means complete) provide updates to the book.
  - The remaining four parts give some references (also not complete) for further reading that are relevant to the topics covered in Chapters One, Two, Three and Four.
- The expanded Notation section now includes all notation used in the book. Specialized notation is listed according to the page where it first appears.

The other changes to the text are very minor, mostly to enhance clarity, improve formatting, and simplify some of the proofs. One exception is the addition of new exercises: at the end of §12, Exercise 12.31 shows how Ramanujan could have derived Weber's formula for $\mathfrak{f}_1(\sqrt{-14})^2$ (thanks to Heng Huat Chan), and at the end of §14, Exercise 14.24 gives an elliptic curve primality test for Mersenne numbers due to Dick Gross [A12] (thanks to Alice Silverberg).

The web site for the book includes typographical errors and a link to supplementary exercises for §§1–3 written by Jeffrey Stopple. The URL of the web site is

`http://www.cs.amherst.edu/~dac/primes.html`

I would like to thank the following people for the errors they found in the first edition and for the suggestions they made: Michael Baake, Dominique Bernardi, Jeff Beyerl, Reinier Bröker, Tony Feng, Nicholas Gavrielides, Lee Goswik, Christian Guenther, Shiv Gupta, Kazuo Hata, Yves Hellegouarach, Norm Hurt, Tim Hutchinson, Trevor Hyde, Maurice Kostas, Susumu Kuninaga, Franz Lemmermeyer, Joseph Lipman, Mario Magioladitis, David May, Stephen Mildenhall, Takashi Ono, Frans Oort, Alf van der Poorten, Jerry Shurman, Alice Silverberg, Neil Sloane, Steve Swanson, Cihangir Tezcan, Satoshi Tomabechi, Fan Xingyuan and Noriko Yui.

Please let me know if you find any errors in the new edition!

My hope is that the second edition of *Primes of the Form* $x^2 + ny^2$ will help bring this wonderful part of number theory to a new audience of students and researchers.

DAVID A. COX

Amherst, Massachsusetts
November 2012

NOTATION

The following standard notation will be used throughout the book.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	The integers, rational numbers, real numbers, and complex numbers
$\mathrm{Re}(z)$, $\mathrm{Im}(z)$	The real and imaginary parts of $z \in \mathbb{C}$
$\mathfrak{h}$	The upper half plane $\{x+iy \in \mathbb{C} : y > 0\}$
$\mathbb{F}_q$	The finite field with q elements
$\mathbb{Z}_p$	The ring of p-adic integers
$\mathbb{Z}/n\mathbb{Z}$	The ring of integers modulo n
$[a] \in A/B$	The coset of $a \in A$ in the quotient A/B
R^*	The group of units in a commutative ring R with identity
$\mathrm{GL}(2,R)$	The group of invertible matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $a,b,c,d \in R$
$\mathrm{SL}(2,R)$	The subgroup of $\mathrm{GL}(2,R)$ of matrices with determinant 1
I	The 2×2 identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
$\mathrm{Gal}(L/K)$	The Galois group of the finite extension $K \subset L$
$[L:K]$	The degree of a the finite extension $K \subset L$
$\mathcal{O}_K$	The ring of algebraic integers in a finite extension K of $\mathbb{Q}$
$\zeta_n = e^{2\pi i/n}$	The standard primitive nth root of unity
$[a,b]$	The set $\{ma+nb : m,n \in \mathbb{Z}\}$
$\gcd(a,b)$	The greatest common divisor of the integers a and b
$\phi(n)$	The Euler ϕ-function
$\log(x)$	The logarithm to the base e of $x \in \mathbb{R}$
$[x]$	The greatest integer $\leq x$ for $x \in \mathbb{R}$
$\lvert S \rvert$	The number of elements in a finite set S
$G \rtimes H$	The semidirect product, where H acts on G
$\ker(\varphi)$, $\mathrm{im}(\varphi)$	The kernel and image of a homomorphism φ
Q.E.D.	The end of a proof or the absence of a proof

Notation for Chapter One

(a/p)	The Legendre symbol	12
(a/m)	The Jacobi symbol	15
$h(D)$	The class number	27
$C(D)$	The class group	45–46
$\chi_i(a)$, $\delta(a)$, $\epsilon(a)$	The assigned characters	49
(P/Q)	The extended Jacobi symbol	66
$\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$	The ring for cubic reciprocity	67
$\mathbb{Z}[i]$, $i = \sqrt{-1}$	The ring of Gaussian integers	67
$N(\alpha)$	The norm of α	67
$(\alpha/\pi)_3$, $(\alpha/\pi)_4$	The cubic and biquadratic Legendre symbols	70, 74
(f, λ)	A Gaussian period	77

Notation for Chapter Two

$N(\mathfrak{a})$	The norm of an ideal	89
I_K, P_K	The groups of ideals and principal ideals of $\mathcal{O}_K$	90
$C(\mathcal{O}_K)$	The ideal class group of $\mathcal{O}_K$	90
$e_{\mathfrak{P}\|\mathfrak{p}}$, $f_{\mathfrak{P}\|\mathfrak{p}}$	The ramification and interial degrees	90
$D_{\mathfrak{P}}$, $I_{\mathfrak{P}}$	The decomposition and inertia groups	91
d_K	The discriminant of K	92
$(D/2)$	The Kronecker symbol	93
$((L/K)/\mathfrak{P})$	The Artin symbol of $\mathfrak{P} \subset \mathcal{O}_L$	95
$((L/K)/\mathfrak{p})$	The Artin symbol of $\mathfrak{p} \subset \mathcal{O}_K$ (Abelian case)	96
$((L/K)/\cdot)$	The Artin map	97
$T(\alpha)$, $N(\alpha)$	The trace and norm of α	104
$\mathcal{O}$	An order in a quadratic field	120
$f = [\mathcal{O}_K : \mathcal{O}]$	The conductor of $\mathcal{O}$	121
$I(\mathcal{O})$, $P(\mathcal{O})$	The groups of ideals and principal ideals of $\mathcal{O}$	123
$C(\mathcal{O})$	The ideal class group of $\mathcal{O}$	123
$h(\mathcal{O})$	The class number of $\mathcal{O}$	124
$C^+(\mathcal{O})$	The narrow (or strict) ideal class group	128
$C_s(\mathcal{O})$	The signed ideal class group	129
$I(\mathcal{O}, f)$, $P(\mathcal{O}, f)$	The $\mathcal{O}$-ideals and principal $\mathcal{O}$-ideals prime to f	130
$I_K(m)$	The $\mathcal{O}_K$-ideals relatively prime to m	130
$P_{K,\mathbb{Z}}(f)$	Subgroup of $I_K(f)$ satisfying $I_K(f)/P_{K,\mathbb{Z}}(f) \simeq C(\mathcal{O})$	131
$\mathfrak{m}$	A modulus in the sense of class field theory	144
$P_{K,1}(\mathfrak{m})$	An important subgroup of $I_K(\mathfrak{m})$	145
$\Phi_{\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$	The Artin map for the modulus $\mathfrak{m}$	145
$\mathfrak{f}(L/K)$	The class field theory conductor of $K \subset L$	146–147
$(\alpha/\mathfrak{p})_n$, $(\alpha/\mathfrak{a})_n$	The nth power Legendre symbols	149
$(\alpha, \beta/\mathfrak{p})_n$	The nth power Hilbert symbol	151
$\mathcal{P}_K$	The set of prime ideals of K	152
$\delta(S)$	The Dirichlet density of $S \subset \mathcal{P}_K$	152
$S \doteq T$	$S \subset T \cup$ finite set	154
$S_{L/K}$, $\tilde{S}_{L/K}$	The primes in K splitting completely in L and variant	154–155
$N_{L/K}$	The norm map from L to K	156–157
$K_{\mathfrak{p}}$	The completion of K at $\mathfrak{p}$	156
$\mathbf{I}_K$, $\mathbf{C}_K$	The idele group and idele class group of K	156
$\Phi_{L/K}$	The idelic Artin map	156

Notation for Chapter Three

$L = [\omega_1, \omega_2]$	A lattice in $\mathbb{C}$	182
$\wp(z) = \wp(z; L)$	The Weierstrass $\wp$-function	182
$g_2(L)$, $g_3(L)$	The coefficients in the differential equation for $\wp$	182–183
$G_r(L)$	The sum $\sum_{\omega \in L - \{0\}} 1/\omega^r$	183
$\Delta(L)$	The discriminant $g_2(L)^3 - 27 g_3(L)^2$	187
e_1, e_2, e_3	The roots of $4x^3 - g_2(L)x - g_3(L)$	187
$j(L)$	The j-invariant of L	188
$j(\tau) = j([1, \tau])$	The j-function of $\tau \in \mathfrak{h}$	190
$j(\mathfrak{a})$	The j-invariant of $\mathfrak{a} \subset \mathcal{O}$	190
$g_2(\tau)$, $g_3(\tau)$	$g_2(L)$, $g_3(L)$ for the lattice $L = [1, \tau]$	200
$\Delta(\tau)$	$\Delta(L)$ for the lattice $L = [1, \tau]$	201
$q = q(\tau)$	The function $e^{2\pi i \tau}$, $\tau \in \mathfrak{h}$	204
$\Gamma_0(m)$	The group $\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z}) : c \equiv 0 \bmod m \right\}$	205
$C(m)$	The matrices that give the cosets of $\Gamma_0(m) \subset \mathrm{SL}(2, \mathbb{Z})$	207
$\Phi_m(X, Y)$	The modular equation	208–209
$h(z; L)$	The Weber function used to generate ray class fields	219
$\Psi(m)$	The cardinality of $C(m)$	223
$\gamma_2(\tau)$	The cube root of the j-function	226
$\gamma_3(\tau)$	The square root of $j(\tau) - 1728$	232
$\eta(\tau)$	The Dedekind η-function	233
$\mathfrak{f}(\tau)$, $\mathfrak{f}_1(\tau)$, $\mathfrak{f}_2(\tau)$	The Weber functions	233
$\sigma(z; \tau)$	The Weierstrass σ-function	234
$\Gamma_0(2)^t$	The transpose of $\Gamma_0(2)$	241
$\zeta(z)$	The Weierstrass ζ-function	252
$H_{\mathcal{O}}(X)$, $H_D(X)$	The class equation	261
$r(\mathcal{O}, m)$	$\lvert\{\alpha \in \mathcal{O} : \alpha \text{ primitive}, N(\alpha) = m\}/\mathcal{O}^*\rvert$	263
$\Phi_{m,1}(X, X)$	The product of the multiplicity one factors of $\Phi_m(X, X)$	266
$J(d_1, d_2)$, $F(n)$	Notation for the Gross–Zagier theorem	274–275

Notation for Chapter Four

E, $E(K)$	An elliptic curve and its group of points over K	284
$\mathbb{P}^2(K)$	The projective plane over the field K	284, 304
$j(E)$	The j-invariant of E	285
$\mathrm{End}_K(E)$	The endomorphism ring of E over K	287, 289
$\deg(\alpha)$	The degree of an isogeny α	288
$Frob_q$	The Frobenius endomorphism of E over $\mathbb{F}_q$	289
$\overline{E}$	The reduction of E modulo a prime	291–292
$H(D)$	The Hurwitz class number	293
$E_0(R)$	The set of points of E over a ring R	298
$\Gamma(m)$	The congruence subgroup $\{\gamma \in \mathrm{SL}(2, \mathbb{Z}) : \gamma \equiv I \bmod m\}$	309
F_m, F	The fields of modular functions of level m and of all levels	309, 311
$f^{\gamma}(\tau)$	The action of the matrix γ on $f(\tau)$	310, 312
$\widehat{\mathbb{Z}}$, $\widehat{\mathbb{Q}}$	The profinite completion of $\mathbb{Z}$ and its tensor product with $\mathbb{Q}$	311
$\mathrm{GL}(2, \mathbb{Q})^+$	The elements of $\mathrm{GL}(2, \mathbb{Q})$ with positive determinant	311
K^{ab}	The maximal Abelian extension of K	312
Φ_K	The idelic Artin map	312, 325
$g_{\tau_0}(x)$	The matrix in $\mathrm{GL}(2, \widehat{\mathbb{Q}})$ associated to $x \in \mathbf{I}_K$	312, 321

$L_{\mathcal{O}}$, $L_{\mathcal{O},m}$	The ring class field and extended ring class field	313
$r(\tau)$	The Rogers–Ramanujan continued fraction	315
$\overline{g}_{\tau_0}(u)$	The matrix in $\mathrm{GL}(2,\mathbb{Z}/m\mathbb{Z})$ associated to $u \in (\mathcal{O}/m\mathcal{O})^*$	317
$\mathcal{O}_p$	The tensor product $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$	319
$\widehat{\mathcal{O}}$, $\widehat{\mathcal{O}}^*$	The ring of adeles and group of ideles over $\mathcal{O}$	319
$\widehat{K}$, $\widehat{K}^*$	The ring of adeles and group of ideles over K	320
$\mathbf{I}_K^{\mathrm{fin}}$	The group of finite ideles of K	325
$K^*\widehat{\mathcal{O}}^*$	The subgroup of $\widehat{K}^*$ that gives $L_{\mathcal{O}}$	326
$J_{\mathcal{O},m} = K^* J^1_{\mathcal{O},m}$	The subgroup of $\widehat{K}^*$ that gives $L_{\mathcal{O},m}$	326
$\mathbf{I}_K^{\mathfrak{m}}$	The subgroup such that $K^*\mathbf{I}_K^{\mathfrak{m}}$ gives the ray class field of $\mathfrak{m}$	331
$\mathbf{I}_K^{\mathrm{fin},\mathfrak{m}}$	Finite version of $\mathbf{I}_K^{\mathfrak{m}}$	331

PRIMES OF THE FORM $x^2 + ny^2$

INTRODUCTION

Most first courses in number theory or abstract algebra prove a theorem of Fermat which states that for an odd prime p,

$$p = x^2 + y^2,\ x,y \in \mathbb{Z} \iff p \equiv 1 \bmod 4.$$

This is only the first of many related results that appear in Fermat's works. For example, Fermat also states that if p is an odd prime, then

$$p = x^2 + 2y^2,\ x,y \in \mathbb{Z} \iff p \equiv 1,3 \bmod 8$$
$$p = x^2 + 3y^2,\ x,y \in \mathbb{Z} \iff p = 3 \text{ or } p \equiv 1 \bmod 3.$$

These facts are lovely in their own right, but they also make one curious to know what happens for primes of the form $x^2 + 5y^2$, $x^2 + 6y^2$, etc. This leads to the basic question of the whole book, which we formulate as follows:

Basic Question 0.1. *Given a positive integer n, which primes p can be expressed in the form*

$$p = x^2 + ny^2$$

where x and y are integers?

We will answer this question completely, and along the way we will encounter some remarkably rich areas of number theory. The first steps will be easy, involving only

quadratic reciprocity and the elementary theory of quadratic forms in two variables over $\mathbb{Z}$. These methods work nicely in the special cases considered above by Fermat. Using genus theory and cubic and biquadratic reciprocity, we can treat some more cases, but elementary methods fail to solve the problem in general. To proceed further, we need class field theory. This provides an abstract solution to the problem, but doesn't give explicit criteria for a particular choice of n in x^2+ny^2. The final step uses modular functions and complex multiplication to show that for a given n, there is an algorithm for answering our question of when $p = x^2+ny^2$.

This book has several goals. The first, to answer the basic question, has already been stated. A second goal is to bridge the gap between elementary number theory and class field theory. Although our basic question is simple enough to be stated in any beginning course in number theory, we will see that its solution is intimately bound up with higher reciprocity laws and class field theory. A related goal is to provide a well-motivated introduction to the classical formulation of class field theory. This will be done by carefully stating the basic theorems and illustrating their power in various concrete situations.

Let us summarize the contents of the book in more detail. We begin in Chapter One with the more elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre and Gauss as a guide. In §1, we will give Euler's proofs of the above theorems of Fermat for primes of the form x^2+y^2, x^2+2y^2 and x^2+3y^2, and we will see what led Euler to discover quadratic reciprocity. We will also discuss the conjectures Euler made concerning $p = x^2+ny^2$ for $n > 3$. Some of these conjectures, such as

$$p = x^2+5y^2 \iff p \equiv 1,9 \bmod 20, \tag{0.2}$$

are similar to Fermat's theorems, while others, like

$$p = x^2+27y^2 \Longleftrightarrow \begin{cases} p \equiv 1 \bmod 3 \text{ and } 2 \text{ is a} \\ \text{cubic residue modulo } p, \end{cases}$$

are quite unexpected. For later purposes, note that this conjecture can be written in the following form:

$$p = x^2+27y^2 \Longleftrightarrow \begin{cases} p \equiv 1 \bmod 3 \text{ and } x^3 \equiv 2 \bmod p \\ \text{has an integer solution.} \end{cases} \tag{0.3}$$

In §2, we will study Lagrange's theory of positive definite quadratic forms. After introducing the basic concepts of reduced form and class number, we will develop an elementary form of genus theory which will enable us to prove (0.2) and similar theorems. Unfortunately, for cases like (0.3), genus theory can only prove the partial result that

$$p = \left\{ \begin{array}{c} x^2+27y^2 \\ \text{or} \\ 4x^2+2xy+7y^2 \end{array} \right\} \Longleftrightarrow p \equiv 1 \bmod 3. \tag{0.4}$$

The problem is that x^2+27y^2 and $4x^2+2xy+7y^2$ lie in the same genus and hence can't be separated by simple congruences. We will also discuss Legendre's tentative attempts at a theory of composition.

While the ideas of genus theory and composition were already present in the works of Lagrange and Legendre, the real depth of these theories wasn't revealed until Gauss came along. In §3 we will present some basic results in Gauss' *Disquisitiones Arithmeticae*, and in particular we will study the remarkable relationship between genus theory and composition. But for our purposes, the real breakthrough came when Gauss used cubic reciprocity to prove Euler's conjecture (0.3) concerning $p=x^2+27y^2$. In §4 we will give a careful statement of cubic reciprocity, and we will explain how it can be used to prove (0.3). Similarly, biquadratic reciprocity can be used to answer our question for x^2+64y^2. We will see that Gauss clearly recognized the role of higher reciprocity laws in separating forms of the same genus. This section will also begin our study of algebraic integers, for in order to state cubic and biquadratic reciprocity, we must first understand the arithmetic of the rings $\mathbb{Z}[e^{2\pi i/3}]$ and $\mathbb{Z}[i]$.

To go further requires class field theory, which is the topic of Chapter Two. We will begin in §5 with the Hilbert class field, which is the maximal unramified Abelian extension of a given number field. This will enable us to prove the following general result:

Theorem 0.5. *Let $n \equiv 1,2 \bmod 4$ be a positive squarefree integer. Then there is an irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that for a prime p dividing neither n nor the discriminant of $f_n(x)$,*

$$p = x^2+ny^2 \iff \begin{cases} (-n/p)=1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

While the statement of Theorem 0.5 is elementary, the polynomial $f_n(x)$ is quite sophisticated: it is the minimal polynomial of a primitive element of the Hilbert class field L of $K=\mathbb{Q}(\sqrt{-n})$.

As an example of this theorem, we will study the case $n=14$. We will show that the Hilbert class field of $K=\mathbb{Q}(\sqrt{-14})$ is $L=K(\alpha)$, where $\alpha=\sqrt{2\sqrt{2}-1}$. By Theorem 0.5, this will show that for an odd prime p,

$$p = x^2+14y^2 \iff \begin{cases} (-14/p)=1 \text{ and } (x^2+1)^2 \equiv 8 \bmod p \\ \text{has an integer solution,} \end{cases} \tag{0.6}$$

which answers our basic question for x^2+14y^2. The Hilbert class field will also enable us in §6 to give new proofs of the main theorems of genus theory.

The theory sketched so far is very nice, but there are some gaps in it. The most obvious is that the above results for x^2+27y^2 and x^2+14y^2 ((0.3) and (0.6) respectively) both follow the same format, but (0.3) does *not* follow from Theorem 0.5, for $n=27$ is *not* squarefree. There should be a unified theorem that works for *all* positive n, yet the proof of Theorem 0.5 breaks down for general n because $\mathbb{Z}[\sqrt{-n}]$ is not in general the full ring of integers in $\mathbb{Q}(\sqrt{-n})$.

The goal of §§7–9 is to show that Theorem 0.5 holds for *all* positive integers n. This, in fact, is the main theorem of the whole book. In §7 we will study the rings $\mathbb{Z}[\sqrt{-n}]$ for general n, which leads to the concept of an *order* in an imaginary quadratic field. In §8 we will summarize the main theorems of class field theory and the Čebotarev Density Theorem, and in §9 we will introduce a generalization of the Hilbert class field called the ring class field, which is a certain (possibly ramified) Abelian extension of $\mathbb{Q}(\sqrt{-n})$ determined by the order $\mathbb{Z}[\sqrt{-n}]$. Then, in Theorem 9.2, we will use the Artin Reciprocity Theorem to show that Theorem 0.5 holds for *all* $n > 0$, where the polynomial $f_n(x)$ is now the minimal polynomial of a primitive element of the above ring class field. To give a concrete example of what this means, we will apply Theorem 9.2 to the case $x^2 + 27y^2$, which will give us a class field theory proof of (0.3). In §§8 and 9 we will also discuss how class field theory is related to higher reciprocity theorems.

The major drawback to the theory presented in §9 is that it is not constructive: for a given $n > 0$, we have no idea how to find the polynomial $f_n(x)$. From (0.3) and (0.6), we know $f_{27}(x)$ and $f_{14}(x)$, but the methods used in these examples hardly generalize. Chapter Three will use the theory of complex multiplication to remedy this situation. In §10 we will study elliptic functions and introduce the idea of complex multiplication, and then in §11 we will discuss modular functions for the group $\Gamma_0(m)$ and show that the j-function can be used to generate ring class fields. As an example of the wonderful formulas that can be proved, in §12 we will give Weber's computation that

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + \left(231 + 161\sqrt{2}\right)\sqrt{2\sqrt{2}-1}\right)^3.$$

These methods will enable us to prove the Baker–Heegner–Stark Theorem on imaginary quadratic fields of class number 1. In §13 of the book we will discuss the class equation, which is the minimal polynomial of $j(\sqrt{-n})$. We will learn how to compute the class equation, which will lead to a constructive solution of $p = x^2 + ny^2$. We will then describe some work by Deuring and by Gross and Zagier. In 1946 Deuring proved a result about the difference of singular j-invariants, which implies an especially elegant version of our main theorem, and drawing on Deuring's work, Gross and Zagier discovered yet more remarkable properties of the class equation.

The first three chapters of the book present a complete solution to the problem of when $p = x^2 + ny^2$. In Chapter Four, we pursue two additional topics, elliptic curves in §14 and Shimura reciprocity in §15, that give a more modern approach to the study of complex multiplication. We also include applications to primality testing in §14. The new §15 discusses ideles and the field of modular functions, and replaces certain pretty but ad-hoc arguments used in §12 with a more systematic treatment based on Shimura reciprocity. We also give an unexpected application to $p = x^2 + ny^2$.

Number theory is usually taught at three levels, as an undergraduate course, a beginning graduate course, or a more advanced graduate course. These levels correspond roughly to the first three chapters of the book. Chapter One requires only beginning number theory (up to quadratic reciprocity) and a semester of abstract algebra. Since the proofs of quadratic, cubic and biquadratic reciprocity are omitted,

this book would be best suited as a supplementary text in a beginning course. For Chapter Two, the reader should know Galois theory and some basic facts about algebraic number theory (these are reviewed in §5), but no previous exposure to class field theory is assumed. The theorems of class field theory are stated without proof, so that this book would be most useful as a supplement to the topics covered in a first graduate course. Chapter Three requires a knowledge of complex analysis, but otherwise it is self-contained. (Brief but complete accounts of the Weierstrass $\wp$-function and modular functions are included in §§10 and 11.) This portion of the book should be suitable for use in a graduate seminar. The same is true for Chapter Four.

There are exercises at the end of each section, many of which consist of working out the details of arguments sketched in the text. Readers learning this material for the first time should find the exercises to be useful, while more sophisticated readers may skip them without loss of continuity.

Many important (and relevant) topics are not covered in the book. An obvious omission in Chapter One concerns forms such as $x^2 - 2y^2$, which were certainly considered by Fermat and Euler. Questions of this sort lead to Pell's equation and the class field theory of real quadratic fields. We have also ignored the problem of representing arbitrary integers, not just primes, by quadratic forms, and there are interesting questions to ask about the *number* of such representations (this material is covered in Grosswald's book [47]). In Chapter Two we give a classical formulation of class field theory, with only a brief mention of adeles and ideles. A more modern treatment can be found in Neukirch [80] or Weil [104] (see also the new §15). We also do not do justice to the use of analytic methods in number theory. For a nice introduction in the case of quadratic fields, see Zagier [111]. Our treatment of elliptic curves in Chapter Four is rather incomplete. See Husemöller [58], Knapp [A14] or Silverman [93] for the basic theory, while more advanced topics are covered by Lang [73], Shimura [90] and Silverman [A21]. At a more elemenary level, there is the wonderful book [A22] by Silverman and Tate.

There are many books which touch on the number theory encountered in studying the problem of representing primes by $x^2 + ny^2$. Four books that we particularly recommend are Cohn's *A Classical Invitation to Algebraic Numbers and Class Fields* [19], Lang's *Elliptic Functions* [73], Scharlau and Opolka's *From Fermat to Minkowski* [86], and Weil's *Number Theory: An Approach Through History* [106]. These books, as well as others to be found in the References, open up an extraordinarily rich area of mathematics. The purpose of this book is to reveal some of this richness and to encourage the reader to learn more about it.

Notes on the Second Edition

The original text of the book consisted of §§1–14. For the second edition, we added the new §15 on Shimura reciprocity described above.

As a supplement to the references for the first edition, a new section *Additional References* has been added. The new references cited in the text are indicated with a leading "A" (e.g., the references Knapp [A14], Silverman [A21], and Silverman and Tate [A22] given above). This section also contains suggestions for further reading for the four chapters.

CHAPTER ONE

FROM FERMAT TO GAUSS

§1. FERMAT, EULER AND QUADRATIC RECIPROCITY

In this section we will discuss primes of the form x^2+ny^2, where n is a fixed positive integer. Our starting point will be the three theorems of Fermat for odd primes p

$$
\begin{aligned}
&p = x^2+y^2,\ x,y\in\mathbb{Z} \iff p\equiv 1 \bmod 4\\
&p = x^2+2y^2,\ x,y\in\mathbb{Z} \iff p\equiv 1 \text{ or } 3 \bmod 8\\
&p = x^2+3y^2,\ x,y\in\mathbb{Z} \iff p=3 \text{ or } p\equiv 1 \bmod 3
\end{aligned}
\tag{1.1}
$$

mentioned in the introduction. The goals of §1 are to prove (1.1) and, more importantly, to get a sense of what's involved in studying the equation $p=x^2+ny^2$ when $n>0$ is arbitrary. This last question was best answered by Euler, who spent 40 years proving Fermat's theorems and thinking about how they can be generalized. Our exposition will follow some of Euler's papers closely, both in the theorems proved and in the examples studied. We will see that Euler's strategy for proving (1.1) was one of the primary things that led him to discover quadratic reciprocity, and we will also discuss some of his remarkable conjectures concerning $p=x^2+ny^2$ for $n>3$.

Primes of the Form x^2+ny^2, Second Edition. By David A. Cox

These conjectures touch on quadratic forms, composition, genus theory, cubic and biquadratic reciprocity, and will keep us busy for the rest of the chapter.

A. Fermat

Fermat's first mention of $p = x^2 + y^2$ occurs in a 1640 letter to Mersenne [35, Vol. II, p. 212], while $p = x^2 + 2y^2$ and $p = x^2 + 3y^2$ come later, first appearing in a 1654 letter to Pascal [35, Vol. II, pp. 310–314]. Although no proofs are given in these letters, Fermat states the results as theorems. Writing to Digby in 1658, he repeats these assertions in the following form:

> Every prime number which surpasses by one a multiple of four is composed of two squares. Examples are 5, 13, 17, 29, 37, 41, etc.
>
> Every prime number which surpasses by one a multiple of three is composed of a square and the triple of another square. Examples are 7, 13, 19, 31, 37, 43, etc.
>
> Every prime number which surpasses by one or three a multiple of eight is composed of a square and the double of another square. Examples are 3, 11, 17, 19, 41, 43, etc.

Fermat adds that he has solid proofs—"firmissimis demonstralibus" [35, Vol. II, pp. 402–408 (Latin), Vol. III, pp. 314–319 (French)].

The theorems (1.1) are only part of the work that Fermat did with $x^2 + ny^2$. For example, concerning $x^2 + y^2$, Fermat knew that a positive integer N is the sum of two squares if and only if the quotient of N by its largest square factor is a product of primes congruent to 1 modulo 4 [35, Vol. III, Obs. 26, pp. 256–257], and he knew the number of different ways N can be so represented [35, Vol. III, Obs. 7, pp. 243–246]. Fermat also studied forms beyond $x^2 + y^2$, $x^2 + 2y^2$ and $x^2 + 3y^2$. For example, in the 1658 letter to Digby quoted above, Fermat makes the following conjecture about $x^2 + 5y^2$, which he admits he can't prove:

> If two primes, which end in 3 or 7 and surpass by three a multiple of four, are multiplied, then their product will be composed of a square and the quintuple of another square.
>
> Examples are the numbers 3, 7, 23, 43, 47, 67, etc. Take two of them, for example 7 and 23; their product 161 is composed of a square and the quintuple of another square. Namely 81, a square, and the quintuple of 16 equal 161.

Fermat's condition on the primes is simply that they be congruent to 3 or 7 modulo 20. In §2 we will present Lagrange's proof of this conjecture, which uses ideas from genus theory and the composition of forms.

Fermat's proofs used the method of infinite descent, but that's often all he said. As an example, here is Fermat's description of his proof for $p = x^2 + y^2$ [35, Vol. II, p. 432]:

> If an arbitrarily chosen prime number, which surpasses by one a multiple of four, is not a sum of two squares, then there is a prime number of the same form, less than the given one, and then yet a third still less, etc., descending infinitely until you arrive at the number 5, which is the least of all of this nature, from which it would follow was not the sum of two squares. From this one must infer, by deduction of the impossible, that all numbers of this form are consequently composed of two squares.

This explains the philosophy of infinite descent, but doesn't tell us how to produce the required lesser prime. We have only one complete proof by Fermat. It occurs in one of his marginal notes (the area of a right triangle with integral sides cannot be an integral square [35, Vol. III, Obs. 45, pp. 271–272]—for once the margin was big enough!). The methods of this proof (see Weil [106, p. 77] or Edwards [31, pp. 10–14] for modern expositions) do not apply to our case, so that we are still in the dark. An analysis of Fermat's approach to infinite descent appears in Bussotti [A5]. Weil's book [106] makes a careful study of Fermat's letters and marginal notes, and with some hints from Euler, he reconstructs some of Fermat's proofs. Weil's arguments are quite convincing, but we won't go into them here. For the present, we prefer to leave things as Euler found them, i.e., wonderful theorems but no proofs.

B. Euler

Euler first heard of Fermat's results through his correspondence with Goldbach. In fact, Goldbach's first letter to Euler, written in December 1729, mentions Fermat's conjecture that $2^{2^n}+1$ is always prime [40, p. 10]. Shortly thereafter, Euler read some of Fermat's letters that had been printed in Wallis' *Opera* [100] (which included the one to Digby quoted above). Euler was intrigued by what he found. For example, writing to Goldbach in June 1730, Euler comments that Fermat's four-square theorem (every positive integer is a sum of four or fewer squares) is a "non inelegans theorema" [40, p. 24]. For Euler, Fermat's assertions were serious theorems deserving of proof, and finding the proofs became a life-long project. Euler's first paper on number theory, written in 1732 at age 25, disproves Fermat's claim about $2^{2^n}+1$ by showing that 641 is a factor of $2^{32}+1$ [33, Vol. II, pp. 1–5]. Euler's interest in number theory continued unabated for the next 51 years—there was a steady stream of papers introducing many of the fundamental concepts of number theory, and even after his death in 1783, his papers continued to appear until 1830 (see [33, Vol. IV–V]). Weil's book [106] gives a survey of Euler's work on number theory (other references are Burkhardt [14], Edwards [31, Chapter 2], Scharlau and Opolka [86, Chapter 3], and the introductions to Volumes II–V of Euler's collected works [33]).

We can now present Euler's proof of the first of Fermat's theorems from (1.1):

Theorem 1.2. *An odd prime p can be written as x^2+y^2 if and only if $p \equiv 1 \bmod 4$.*

Proof. If $p = x^2+y^2$, then congruences modulo 4 easily imply that $p \equiv 1 \bmod 4$. The hard work is proving the converse. We will give a modern version of Euler's proof. Given an odd prime p, there are two basic steps to be proved:

$$\begin{aligned} &\textit{Descent Step}: \text{If } p \mid x^2+y^2,\ \gcd(x,y)=1, \text{ then } p \text{ can be written} \\ &\qquad\qquad \text{as } x^2+y^2 \text{ for some possibly different } x,\ y. \\ &\textit{Reciprocity Step}: \text{If } p \equiv 1 \bmod 4, \text{ then } p \mid x^2+y^2,\ \gcd(x,y)=1. \end{aligned}$$

It will soon become clear why we use the names "Descent" and "Reciprocity."

We'll do the Descent Step first since that's what happened historically. The argument below is taken from a 1747 letter to Goldbach [40, pp. 416–419] (see also [33,

Vol. II, pp. 295–327]). We begin with the classical identity

$$(x^2+y^2)(z^2+w^2) = (xz \pm yw)^2 + (xw \mp yz)^2 \tag{1.3}$$

(see Exercise 1.1) which enables one to express composite numbers as sums of squares. The key observation is the following lemma:

Lemma 1.4. *Suppose that N is a sum of two relatively prime squares, and that $q = x^2+y^2$ is a prime divisor of N. Then N/q is also a sum of two relatively prime squares.*

Proof. Write $N = a^2+b^2$, where a and b are relatively prime. We also have $q = x^2+y^2$, and thus q divides

$$\begin{aligned} x^2N - a^2q &= x^2(a^2+b^2) - a^2(x^2+y^2) \\ &= x^2b^2 - a^2y^2 = (xb-ay)(xb+ay). \end{aligned}$$

Since q is prime, it divides one of these two factors, and changing the sign of a if necessary, we can assume that $q \mid xb-ay$. Thus $xb-ay = dq$ for some integer d.

We claim that $x \mid a+dy$. Since x and y are relatively prime, this is equivalent to $x \mid (a+dy)y$. However,

$$\begin{aligned} (a+dy)y &= ay+dy^2 = xb-dq+dy^2 \\ &= xb - d(x^2+y^2)+dy^2 = xb-dx^2, \end{aligned}$$

which is obviously divisible by x. Furthermore, if we set $a+dy = cx$, then the above equation implies that $b = dx+cy$. Thus we have

$$\begin{aligned} a &= cx-dy \\ b &= dx+cy. \end{aligned} \tag{1.5}$$

Then, using (1.3), we obtain

$$\begin{aligned} N = a^2+b^2 &= (cx-dy)^2+(dx+cy)^2 \\ &= (x^2+y^2)(c^2+d^2) = q(c^2+d^2). \end{aligned}$$

Thus $N/q = c^2+d^2$ is a sum of squares, and (1.5) shows that c and d must be relatively prime since a and b are. This proves the lemma. Q.E.D.

To complete the proof of the Descent Step, let p be an odd prime dividing $N = a^2+b^2$, where a and b are relatively prime. If a and b are changed by multiples of p, we still have $p \mid a^2+b^2$. We may thus assume that $|a| < p/2$ and $|b| < p/2$, which in turn implies that $N < p^2/2$. The new a and b may have a greatest common divisor $d > 1$, but p doesn't divide d, so that dividing a and b by d, we may assume that $p \mid N$, $N < p^2/2$, and $N = a^2+b^2$ where $\gcd(a,b) = 1$. Then all prime divisors $q \neq p$ of N are less than p. If q were a sum of two squares, then Lemma 1.4 would show that N/q would be a multiple of p that is again a sum of two squares. If all such

q's were sums of two squares, then repeatedly applying Lemma 1.4 would imply that p itself was of the same form. So if p is not a sum of two squares, there must be a smaller prime q with the same property. Since there is nothing to prevent us from repeating this process indefinitely, we get an infinite decreasing sequence of prime numbers. This contradiction finishes the Descent Step.

This is a classical descent argument, and as Weil argues [106, pp. 68–69], it is probably similar to what Fermat did. In §2 we will take another approach to the Descent Step, using the reduction theory of positive definite quadratic forms.

The Reciprocity Step caused Euler a lot more trouble, taking him until 1749. Euler was clearly relieved when he could write to Goldbach "Now have I finally found a valid proof" [40, pp. 493–495]. The basic idea is quite simple: since $p \equiv 1 \bmod 4$, we can write $p = 4k+1$. Then Fermat's Little Theorem implies that

$$(x^{2k}-1)(x^{2k}+1) \equiv x^{4k}-1 \equiv 0 \bmod p$$

for all $x \not\equiv 0 \bmod p$. If $x^{2k}-1 \not\equiv 0 \bmod p$ for *one* such x, then $p \mid x^{2k}+1$, so that p divides a sum of relatively prime squares, as desired. For us, the required x is easy to find, since $x^{2k}-1$ is a polynomial over the field $\mathbb{Z}/p\mathbb{Z}$ and hence has at most $2k < p-1$ roots. Euler's first proof is quite different, for it uses the calculus of finite differences—see Exercise 1.2 for details. This proves Fermat's claim (1.1) for primes of the form x^2+y^2. Q.E.D.

Euler used the same two-step strategy in his proofs for x^2+2y^2 and x^2+3y^2. The Descent Steps are

$$\begin{aligned} &\text{If } p \mid x^2+2y^2,\ \gcd(x,y)=1, \text{ then } p \text{ is of the form } x^2+2y^2 \text{ for} \\ &\qquad\qquad \text{some possibly different } x,\ y \\ &\text{If } p \mid x^2+3y^2,\ \gcd(x,y)=1, \text{ then } p \text{ is of the form } x^2+3y^2 \text{ for} \\ &\qquad\qquad \text{some possibly different } x,\ y, \end{aligned}$$

and the Reciprocity Steps are

$$\begin{aligned} &\text{If } p \equiv 1,3 \bmod 8, \text{ then } p \mid x^2+2y^2,\ \gcd(x,y)=1 \\ &\text{If } p \equiv 1 \bmod 3, \text{ then } p \mid x^2+3y^2,\ \gcd(x,y)=1, \end{aligned}$$

where p is always an odd prime. In each case, the Reciprocity Step was harder to prove than the Descent Step, and Euler didn't succeed in giving complete proofs of Fermat's theorems (1.1) until 1772, 40 years after he first read about them. Weil discusses the proofs for x^2+2y^2 and x^2+3y^2 in [106, pp. 178–179, 191, and 210–212], and in Exercises 1.4 and 1.5 we will present a version of Euler's argument for x^2+3y^2.

C. $p = x^2 + ny^2$ and Quadratic Reciprocity

Let's turn to the general case of $p = x^2+ny^2$, where n is now any positive integer. To study this problem, it makes sense to start with Euler's two-step strategy. This won't