**Theorem 5.1.** *Let $n > 0$ be an integer satisfying the following condition:*

$$n \text{ squarefree}, \quad n \not\equiv 3 \bmod 4. \tag{5.2}$$

*Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime $p$ divides neither $n$ nor the discriminant of $f_n(x)$, then*

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

*Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer $\alpha$ for which $L = K(\alpha)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$.*

While (5.2) does not give all integers $n > 0$, it gives infinitely many, so that Theorem 5.1 represents some real progress. In §9 we will use the full power of class field theory to prove a version of Theorem 5.1 that holds for *all* positive integers $n$.

## A. Number Fields

We will review some basic facts from algebraic number theory, including Dedekind domains, factorization of ideals, and ramification. Most of the proofs will be omitted, though references will be given. Readers looking for a more complete treatment should consult Borevich and Shafarevich [8], Lang [72] or Marcus [77]. For an especially compact presentation of this material, see Ireland and Rosen [59, Chapter 12].

To begin, we define a *number field* $K$ to be a subfield of the complex numbers $\mathbb{C}$ which has finite degree over $\mathbb{Q}$. The degree of $K$ over $\mathbb{Q}$ is denoted $[K : \mathbb{Q}]$. Given such a field $K$, we let $\mathcal{O}_K$ denote the algebraic integers of $K$, i.e., the set of all $\alpha \in K$ which are roots of a monic integer polynomial. The basic structure of $\mathcal{O}_K$ is given in the following proposition:

**Proposition 5.3.** *Let $K$ be a number field.*

(i) *$\mathcal{O}_K$ is a subring of $\mathbb{C}$ whose field of fractions is $K$.*

(ii) *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

*Proof.* See Borevich and Shafarevich [8, §2.2] or Marcus [77, Corollaries to Theorems 2 and 9]. Q.E.D.

We will often call $\mathcal{O}_K$ the number ring of $K$. To begin our study of $\mathcal{O}_K$, we note that part (ii) of Proposition 5.3 has the following useful consequence concerning the ideals of $\mathcal{O}_K$:



**Corollary 5.4.** *If $K$ is a number field and $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$, then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.*

*Proof.* See Exercise 5.1. Q.E.D.

Given a nonzero ideal $\mathfrak{a}$ of the number ring $\mathcal{O}_K$, its *norm* is defined to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. Corollary 5.4 guarantees that $N(\mathfrak{a})$ is finite.

When we studied the rings $\mathbf{Z}[\omega]$ and $\mathbf{Z}[i]$ in §4, we used the fact that they were unique factorization domains. In general, the rings $\mathcal{O}_K$ are not UFDs, but they have another property which is almost as good: they are Dedekind domains. This means the following:

**Theorem 5.5.** *Let $\mathcal{O}_K$ be the ring of integers in a number field $K$. Then $\mathcal{O}_K$ is a Dedekind domain, which means that*

(i) *$\mathcal{O}_K$ is integrally closed in $K$, i.e., if $\alpha \in K$ satisfies a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.*

(ii) *$\mathcal{O}_K$ is Noetherian, i.e., given any chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, there is an integer $n$ such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.*

(iii) *Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

*Proof.* The proof of (i) follows easily from the properties of algebraic integers (see Lang [72, §I.2] or Marcus [77, Exercise 4 to Chapter 2]), while (ii) and (iii) are straightforward consequences of Corollary 5.4 (see Exercise 5.1). Q.E.D.

The most important property of a Dedekind domain is that it has unique factorization at the level of ideals. More precisely:

**Corollary 5.6.** *If $K$ is a number field, then any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as a product*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

*of prime ideals, and the decomposition is unique up to order. Furthermore, the $\mathfrak{p}_i$'s are exactly the prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$.*

*Proof.* This corollary holds for any Dedekind domain. For a proof, see Lang [72, §I.6] or Marcus [77, Chapter 3, Theorem 16]. In Ireland and Rosen [59, §12.2] there is a nice proof (due to Hurwitz) that is special to the number field case. Q.E.D.

Prime ideals play an especially important role in algebraic number theory. We will often say "prime" rather than "nonzero prime ideal", and the

(recall that $P_{K,\mathbf{Z}}(f)$ is generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer $a$ with $\gcd(a,f) = 1$). Furthermore, in §8 we saw that

$$P_{K,1}(f) \subset P_{K,\mathbf{Z}}(f) \subset I_K(f),$$

so that $C(\mathcal{O})$ is a generalized ideal class group of $K$ for the modulus $f\mathcal{O}_K$ (see (8.1)). By the Existence Theorem (Theorem 8.6), this data determines a unique Abelian extension $L$ of $K$, which is called the *ring class field* of the order $\mathcal{O}$. The basic properties of the ring class field $L$ are, first, all primes of $K$ ramified in $L$ must divide $f\mathcal{O}_K$, and second, the Artin map and (9.1) give us isomorphisms

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbf{Z}}(f) \simeq \mathrm{Gal}(L/K).$$

In particular the degree of $L$ over $K$ is the class number, i.e., $[L:K] = h(\mathcal{O})$. For an example of a ring class field, note that the ring class field of the maximal order $\mathcal{O}_K$ is the Hilbert class field of $K$ (see Exercise 9.1). Later in this section we will give other examples of ring class fields.

We can now state the main theorem of the book:

**Theorem 9.2.** *Let $n > 0$ be an integer. Then there is a monic irreducible polynomial $f_n(x) \in \mathbf{Z}[x]$ of degree $h(-4n)$ such that if an odd prime $p$ divides neither $n$ nor the discriminant of $f_n(x)$, then*

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

*Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer $\alpha$ for which $L = K(\alpha)$ is the ring class field of the order $\mathbf{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-n})$.*

*Finally, if $f_n(x)$ is any monic integer polynomial of degree $h(-4n)$ for which the above equivalence holds, then $f_n(x)$ is irreducible over $\mathbf{Z}$ and is the minimal polynomial of a primitive element of the ring class field $L$ described above.*

***Remark.*** This theorem generalizes Theorem 5.1, and the last part of the theorem shows that knowing $f_n(x)$ is *equivalent* to knowing the ring class field of $\mathbf{Z}[\sqrt{-n}]$.

*Proof.* Before proceeding with the proof, we will first prove the following general fact about ring class fields:

**Lemma 9.3.** *Let $L$ be the ring class field of an order $\mathcal{O}$ in an imaginary quadratic field $K$. Then $L$ is a Galois extension of $\mathbf{Q}$, and its Galois group can be written as a semidirect product*

$$\mathrm{Gal}(L/\mathbf{Q}) \simeq \mathrm{Gal}(L/K) \rtimes (\mathbf{Z}/2\mathbf{Z})$$



*where the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$ acts on $\mathrm{Gal}(L/K)$ by sending $\sigma$ to its inverse $\sigma^{-1}$.*

*Proof.* In the case of the Hilbert class field, this lemma was proved in §6 (see the discussion following (6.3)). To do the general case, we first need to show that $\tau(L) = L$, where $\tau$ denotes complex conjugation. Let $\mathfrak{m}$ denote the modulus $f\mathcal{O}_K$, and note that $\tau(\mathfrak{m}) = \mathfrak{m}$. Since $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbf{Z}}(f)$, an easy computation shows that

$$\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \tau(\ker(\Phi_{L/K,\mathfrak{m}})) = \tau(P_{K,\mathbf{Z}}(f)) = P_{K,\mathbf{Z}}(f)$$

(see Exercise 9.2), and thus $\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}})$. Then $\tau(L) = L$ follows from Corollary 8.7.

As we noticed in the proof of Lemma 5.28, this implies that $L$ is Galois over $\mathbf{Q}$, so that we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow \mathrm{Gal}(K/\mathbf{Q})(\simeq \mathbf{Z}/2\mathbf{Z}) \longrightarrow 1.$$

Since $\tau \in \mathrm{Gal}(L/\mathbf{Q})$, $\mathrm{Gal}(L/\mathbf{Q})$ is the semidirect product $\mathrm{Gal}(L/K) \rtimes (\mathbf{Z}/2\mathbf{Z})$, where the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$ acts by conjugation by $\tau$. However, for a prime $\mathfrak{p}$ of $K$, Lemma 5.19 implies that

$$\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1} = \left(\frac{L/K}{\tau(\mathfrak{p})}\right) = \left(\frac{L/K}{\bar{\mathfrak{p}}}\right)$$

(see Exercise 6.3). Thus, under the isomorphism $I_K(f)/P_{K,\mathbf{Z}}(f) \simeq \mathrm{Gal}(L/K)$, conjugation by $\tau$ in $\mathrm{Gal}(L/K)$ corresponds to the usual action of $\tau$ on $I_K(f)$. But if $\mathfrak{a}$ is any ideal in $I_K(f)$, then $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}_K$ lies in $P_{K,\mathbf{Z}}(f)$ since $N(\mathfrak{a})$ is prime to $f$. Thus $\bar{\mathfrak{a}}$ gives the *inverse* of $\mathfrak{a}$ in the quotient $I_K(f)/P_{K,\mathbf{Z}}(f)$, and the lemma is proved. Q.E.D.

We can now proceed with the proof of Theorem 9.2. Let $L$ be the ring class field of $\mathbf{Z}[\sqrt{-n}]$. We start by relating $p = x^2 + ny^2$ to the behavior of $p$ in $L$:

**Theorem 9.4.** *Let $n > 0$ be an integer, and $L$ be the ring class field of the order $\mathbf{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-n})$. If $p$ is an odd prime not dividing $n$, then*

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

*Proof.* Let $\mathcal{O} = \mathbf{Z}[\sqrt{-n}]$. The discriminant of $\mathcal{O}$ is $-4n$, and then $-4n = f^2 d_K$ by (7.3), where $f$ is the conductor of $\mathcal{O}$. Let $p$ be an odd prime not dividing $n$. Then $p \nmid f^2 d_K$, which implies that $p$ is unramified in $K$. We will

*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
p. cm.
Bibliography: p.
Includes index.
1. Numbers, Prime. I. Title. II. Title: Primes of the form $x^2$ plus $ny^2$.
QA246.C69 1989
512'.72—dc19 89-5555
ISBN 0-471-50654-0
ISBN 0-471-19079-9 (paperback)

Printed in the United States of America

10 9 8 7 6 5 4 3

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

## Fermat, Class Field Theory, and Complex Multiplication

**David A. Cox**
Department of Mathematics
Amherst College
Amherst, Massachusetts

A WILEY-INTERSCIENCE PUBLICATION

**JOHN WILEY & SONS, INC.**

New York / Chichester / Weinheim / Brisbane / Singapore / Toronto