Class field theory, lattices with complex multiplication, and the form $x^2 + ny^2$

Anthony Várilly

Harvard University, Cambridge, MA 02138
Math 251r: Arithmetic Theory of Quadratic forms, Spring 2003

Abstract

We prove, using class field theory, that there is an algorithm to determine which rational primes p are represented by the form $x^2 + ny^2$ ($n > 0$). Then, with the aid of lattices that admit complex multiplication, we briefly show how one may implement this algorithm.

1 Introduction

It is in general hard to determine which positive integers can be represented by a positive definite binary quadratic form with integer matrix. In this paper we focus on the form x^2+ny^2 ($n > 0$) and give an algorithm to determine whether a rational prime p is represented by this form. We will first show that such an algorithm exists by using the full force of the class field theory of imaginary quadratic fields. Then we will briefly outline how one may use lattices that admit complex multiplication to make explicit the criterion furnished by class field theory.

2 Class Field Theory

We begin the paper with a quick summary of the necessary class field theory to study which primes are of the form $x^2 + ny^2$. The reader wishing to find proofs of the theorems stated in this section might look at [Neu], [Jan] or [Lang], for example. We will follow a mixture between the presentations of [Sil 2, §II.3] and [Cox, §8] in our exposition.

Unless otherwise stated, K will be a totally imaginary field, i.e., a field with no real embeddings. This means we can forget about the real infinite primes of K, which will make the definitions and the theorems of class field theory easier to state. We note that a quadratic imaginary field is totally imaginary, and since we are only concerned with the class field theory of such fields we lose nothing by making this extra assumption about our ground field.

Let L be a finite abelian extension of K (that is, a finite Galois extension with abelian Galois group), and denote the rings of integers of these fields by $\mathcal{O}_L$ and $\mathcal{O}_K$, respectively. Let $\mathfrak{p}$ be an prime in $\mathcal{O}_K$ unramified in $\mathcal{O}_L$ and $\mathfrak{P}$ be a prime in $\mathcal{O}_L$ lying over $\mathfrak{p}$. Recall $\mathcal{O}_L/\mathfrak{P}$ is a finite extension of $\mathcal{O}_K/\mathfrak{p}$; we will write $f_{\mathfrak{P}/\mathfrak{p}}$ for the degree of this extension.

Lemma 1. *With the preceding notation, there is a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}, \tag{1}$$

where $N(\mathfrak{p}) = N_{\mathbb{Q}}^{K}(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p}$.

Proof. Let $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ denote the decomposition and inertia groups of $\mathfrak{P}$, respectively. Explicitly,

$$\begin{aligned} D_{\mathfrak{P}} &= \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathfrak{P}) = \mathfrak{P}\}, \\ I_{\mathfrak{P}} &= \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(x) \equiv x \bmod \mathfrak{P} \ \ \forall\, x \in \mathcal{O}_L\}. \end{aligned}$$

Clearly, an element $\sigma \in D_{\mathfrak{P}}$ induces an element $\bar{\sigma} \in \overline{G} := \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P}) \,/\, (\mathcal{O}_K/\mathfrak{p}))$. It is well known that $I_{\mathfrak{P}}$ is a normal subgroup of $D_{\mathfrak{P}}$ and that $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is isomorphic to $\overline{G}$ [Mar, p.101]. Since $\mathfrak{p}$ is unramified, $\#I_{\mathfrak{P}} = e_{\mathfrak{P}|\mathfrak{p}} = 1$, so that $D_{\mathfrak{P}}$ is isomorphic to $\overline{G}$. We know, however, that $\overline{G}$ is cyclic, generated by the Frobenius automorphism $x \to x^{N(\mathfrak{p})}$. We conclude there is a $\sigma \in D_{\mathfrak{P}}$ that maps to this element, i.e., for all $\alpha \in \mathcal{O}_L$

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

It is not hard to show that any σ satisfying (1) must be in $D_{\mathfrak{P}}$, from which the uniqueness of σ follows. □

Note that the relation (1) can be extended to $\alpha \in L$, by which we mean that $\sigma(\alpha) - \alpha^{N(\mathfrak{p})}$ has positive $\mathfrak{P}$-adic valuation. We call the unique σ in the above lemma the *Artin symbol* and denote it $((L/K)/\mathfrak{P})$. From its uniqueness we deduce that for $\sigma \in \mathrm{Gal}(L/K)$

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1},$$

so if $\mathrm{Gal}(L/K)$ is abelian, the Artin symbol is determined by $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ because $\mathrm{Gal}(L/K)$ acts transitively on the set of primes that lie above $\mathfrak{p}$. In this case, we will denote the symbol $((L/K)/\mathfrak{p})$.

Remark 2. As above, if $\mathfrak{p}$ is a prime of K unramified in L, then $D_{\mathfrak{P}} \cong \overline{G}$. Since $\#\overline{G} = f_{\mathfrak{P}/\mathfrak{p}}$, we conclude the Artin symbol $((L/K)/\mathfrak{p})$ has order $f_{\mathfrak{P}/\mathfrak{p}}$. Now, an unramified prime $\mathfrak{p}$ splits completely in L if and only if $f_{\mathfrak{P}/\mathfrak{p}} = 1$. Hence $\mathfrak{p}$ splits completely if and only if the Artin symbol is the identity element of $\mathrm{Gal}(L/K)$. This means that the unramified primes in the kernel of the Artin Map are those primes of K that split completely in L.

Definition 1. *Let K be a total imaginary field. A* modulus $\mathfrak{m}$ *in K is a formal product over all primes $\mathfrak{p} \in \mathcal{O}_K$*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

where the $n_{\mathfrak{p}}$ are non-negative integers only finitely many of which are non-zero. If $n_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, then we set $\mathfrak{m} = 1$.

Let $I(\mathfrak{m})$ be the group of fractional ideals in $\mathcal{O}_K$ that are relatively prime to $\mathfrak{m}$, and let $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$ be an ideal in $I(\mathfrak{m})$. If $\mathfrak{m}$ is divisible by all primes of K that ramify in L, we can define the *Artin map* through the Artin symbol, extended by linearity as follows

$$\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} : I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$
$$\left(\frac{L/K}{\mathfrak{a}}\right)_{\mathfrak{m}} := \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

We can now state a weak version of the Artin reciprocity theorem.

Theorem 3 (Artin Reciprocity). *Let L be an abelian extension of a totally imaginary field K. Then there exists a modulus $\mathfrak{m}$ of K divisible by precisely those primes of K that ramify in L such that*

$$\left(\frac{L/K}{(\alpha)}\right)_{\mathfrak{m}} = 1 \quad \textit{for all } \alpha \in K^* \textit{ such that } \alpha \equiv 1 \bmod \mathfrak{m}.$$

If the theorem is true for two moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$ then it is true for their sum $\mathfrak{m}_1 + \mathfrak{m}_2$, so there is a largest modulus for which Artin Reciprocity is true. We call this modulus the *conductor* of L/K and denote it $\mathfrak{c}_{L/K}$. An important theorem of CFT asserts the existence of a maximal abelian extension $K_{\mathfrak{m}}$ of K with conductor $\mathfrak{m}$. This extension is called a *ray class field* of K for the modulus $\mathfrak{m}$. More precisely,

Definition 2. *Let $\mathfrak{m}$ be a modulus of K. A* ray class field *of K for the modulus $\mathfrak{m}$ is a finite abelian extension $K_{\mathfrak{m}}/K$ such that for any other finite abelian extension L/K*

$$\mathfrak{c}_{L/K} | \mathfrak{m} \implies L \subset K_{\mathfrak{m}}.$$

The simplest example of a ray class field is obtained by setting $\mathfrak{m} = 1$. The field thus obtained is the maximal unramified abelian extension of K. It is known as the *Hilbert Class Field* of K.

In view of the weak Reciprocity theorem above, it is natural for us to consider the group $P(\mathfrak{m})$ of principal ideals of $\mathcal{O}_K$ congruent to 1 modulo $\mathfrak{m}$

$$P(\mathfrak{m}) = \{(\alpha) \,|\, \alpha \in K^*, \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

Note that for (α) to belong to $P(\mathfrak{m})$ we only require there exist $\zeta \in \mathcal{O}_K^*$ such that $\zeta\alpha \equiv 1 \bmod \mathfrak{m}$.

It is true that $P(\mathfrak{m})$ has finite index in $I(\mathfrak{m})$ [Cox, p.160]. A group G is called a *congruence subgroup* if

$$P(\mathfrak{m}) \subset G \subset I(\mathfrak{m})$$

and $I(\mathfrak{m})/G$ is called a *generalized ideal class group* for the modulus $\mathfrak{m}$. The key theme of CFT is that generalized ideal class groups are the Galois groups of abelian extensions of the ground field K, and the link between these two kinds of groups is provided by the Artin map. We may restate Theorem 3 as follows.

Theorem 4 (Artin Reciprocity). *Let L/K be a finite abelian extension, then there is a modulus $\mathfrak{c}_{L/K}$, divisible precisely by the ramified primes of K and such that the Artin Map*

$$\left(\frac{L/K}{\cdot}\right)_{\mathfrak{c}_{L/K}} : I(\mathfrak{c}_{L/K}) \to \mathrm{Gal}(L/K)$$

is a surjective homomorphism. Its kernel G is a congruence group for the conductor $\mathfrak{c}_{L/K}$, and thus $\mathrm{Gal}(L/K) \cong I(\mathfrak{c}_{L/K})/G$ is a generalized ideal class group for the modulus $\mathfrak{c}_{L/K}$.

The following theorem asserts that every generalized ideal class group is a Galois group for some abelian extension L/K.

Theorem 5 (Existence Theorem). *Let $\mathfrak{m}$ be a modulus for K and let G be a congruence subgroup for $\mathfrak{m}$. Then there is an abelian extension L/K, all of whose ramified primes divide $\mathfrak{m}$ such that G is the kernel of the Artin map*

$$\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} : I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

Example 1. Consider the modulus $\mathfrak{m} = f\mathcal{O}_K$, where f is the conductor of an order $\mathcal{O}$ in an imaginary quadratic field K. Recall there is an abelian group $C(\mathcal{O})$ attached to every order called the order class group. It is the quotient of proper fractional $\mathcal{O}$-ideals $I(\mathcal{O})$ by principal $\mathcal{O}$-ideals. Let $I_K(f)$ denote the *group* of $\mathcal{O}_K$-ideals that are prime to the conductor f, i.e., $\mathcal{O}_K$-ideals $\mathfrak{a}$ such that $\mathfrak{a} + f\mathcal{O}_K = \mathcal{O}_K$, or equivalently, $\gcd(N(\mathfrak{a}), f) = 1$. Now let $P_K(f)$ be the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ and $\alpha \equiv a \bmod f\mathcal{O}_K$ for an integer a relatively prime to f. There is an isomorphism

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \cong I_K(f)/P_K(f), \tag{2}$$

see, for example, [Cox, Prop. 7.22]. We also have inclusions

$$P(f\mathcal{O}_K) \subset P_K(f) \subset I_K(f) = I(f\mathcal{O})$$

which show $C(\mathcal{O})$ is a generalized ideal class group of K for the modulus $f\mathcal{O}_K$. By Theorem 5 there is an abelian extension L/K, called the *ring class field* of the order $\mathcal{O}$, such that the ramified primes of K in L divide $f\mathcal{O}_K$. Furthermore, the Artin map gives an isomorphism

$$C(\mathcal{O}) \cong I_K(f)/P_K(f) \cong \mathrm{Gal}(L/K).$$

The following corollary of Theorem 5, whose proof we omit (see [Cox, Corollary 8.7]) will be of great use for us.

Corollary 6. *Let L and M be two abelian extensions of K. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all the ramified primes of K in L or M, such that*

$$P(\mathfrak{m}) \subset \ker\left(\left(\frac{M/K}{\cdot}\right)_{\mathfrak{m}}\right) \subset \ker\left(\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}\right)$$

3 A nonconstructive criterion

Let K be a quadratic imaginary field with number ring $\mathcal{O}_K$. Let $\mathcal{O}$ be an order in K of conductor f, so that $[1, fw_k]$ is a $\mathbb{Z}$-basis for $\mathcal{O}$, where $w_k = (d_K + \sqrt{d_K})/2$ and d_K is the discriminant of K. We denote the size of the order class group $\#C(\mathcal{O})$ by $h(\mathrm{disc}(\mathcal{O}))$.

We want to give a criterion to determine when a prime p is of the form $x^2 + ny^2$. This is the content of the following theorem:

Theorem 7. *Let n be a positive integer. 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*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\dfrac{-n}{p}\right) = 1 \text{ and } f_n(X) \equiv 0 \bmod p \\ \text{has a solution for some } x \in \mathbb{Z}. \end{cases}$$

Moreover, the polynomial f_n can be the minimal polynomial of a real algebraic integer which is a primitive element α for the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in $K = \mathbb{Q}(\sqrt{-n})$.

We remark that Theorem 7 does not explicitly give the polynomial $f_n(X)$, it merely asserts that the polynomial exists. We will come back to point in the next section.

We begin our task of proving Theorem 7 by proving the following:

Theorem 8. *Let L be the ring class field of $\mathbb{Z}[\sqrt{-n}]$ ($n > 0$). Suppose p is an odd prime that does not divide n. Then $p = x^2 + ny^2$ if and only if p splits completely in L.*

Proof. The discriminant of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ is $-4n$. Since p is odd and does not divide n we conclude $p \nmid \operatorname{disc} \mathcal{O}$, which is to say that p is unramified in K.

We claim that

$$p = x^2 + ny^2 \iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}, \text{ and } \mathfrak{p} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O}.$$

Indeed, suppose $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Let $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$, so that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Then $\mathfrak{p} \neq \overline{\mathfrak{p}}$ because p is unramified in K. Conversely, if $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}$ and $\mathfrak{p} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O}$ then we can set $\alpha = x + \sqrt{-n}y$ for some integers x and y and consequently $p = x^2 + ny^2$.

Now, to say that $\mathfrak{p} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}$ is equivalent to the assertion that $\mathfrak{p} \in P_K(f)$. On the one hand, if $\mathfrak{p} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}$, we know that $\mathfrak{p} + f\mathcal{O}_K = \mathcal{O}_K$ because $\gcd(p, f) = 1$, so $\mathfrak{p}$ is certainly in $I_K(f)$ (see Example 1). Since $\alpha \in \mathcal{O} = [1, fw_K]$ we see that $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a. Furthermore, we know $N(\alpha) = p$, and so $\gcd(N(\alpha), f) = 1$; it is clear that $N(\alpha) \equiv a^2 \bmod f\mathcal{O}_K$, from which we conclude that $\gcd(a, f) = 1$. Hence $\mathfrak{p} \in P_K(f)$. On the other hand, if $\mathfrak{p} \in P_K(f)$ we know that $\mathfrak{p} = \alpha\mathcal{O}_K$ and $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a which is relatively prime to f. Since $\mathcal{O} = [1, fw_K]$ and $\alpha = a + fw$ for some $w \in \mathcal{O}_K$ it follows that $\alpha \in \mathcal{O}$.

From this equivalence we infer that

$$p = x^2 + ny^2 \iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}, \text{ and } \mathfrak{p} \in P_K(f).$$

Since $C(\mathcal{O})$ is a generalized ideal class group for the modulus $f\mathcal{O}_K$, the Artin map gives a surjective homomorphism

$$I_K(f) \to \operatorname{Gal}(L/K)$$

(see Example 1). However, since $C(\mathcal{O}) \cong I_K(f)/P_K(f)$, it follows that

$$\mathfrak{p} \in P_K(f) \iff \left(\frac{L/K}{\mathfrak{p}}\right) = 1.$$

but the Artin symbol is trivial if and only if $\mathfrak{p}$ splits completely in L (see Remark 2). Hence

$$p = x^2 + ny^2 \iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}, \text{ and } \mathfrak{p} \text{ splits completely in } L.$$

It remains to show that

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}, \text{ and } \mathfrak{p} \text{ splits completely in } L \iff p \text{ splits completely in } L.$$

Suppose that L is a Galois extension of $\mathbb{Q}$. If $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ splits completely in K and $\mathfrak{p}$ splits completely in L then

$$p\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_m\overline{\mathfrak{p}},$$

where $\mathfrak{P}_i$ are the distinct prime factors of $\mathfrak{p}$ in L. Say $\overline{\mathfrak{p}}$ factors as $\mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_n'^{e_n}$. Then the full factorization of p in $\mathcal{O}_L$ would be

$$p\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_m\mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_n'^{e_n}.$$

But if L is Galois over $\mathbb{Q}$ the ramification indices and the inertia degrees of the primes of L above p are all equal (this a general property of number fields), i.e., $e_1 = \cdots = e_n = 1$ and $[\mathcal{O}_L/\mathfrak{P} : \mathbb{F}_p] = 1$ for each $\mathfrak{P} \in L$ above p. This means p splits completely in $\mathbb{Q}$. The converse implication is clear.

It remains to show that L is Galois over $\mathbb{Q}$; we do this in a separate, slightly more general Lemma below. □

Lemma 9. *Let L be the ring class field of an order $\mathcal{O}$ in a quadratic imaginary field K. Then L is a Galois extension of $\mathbb{Q}$.*

Proof. Let τ denote complex conjugation and set $[L : K]$. The extension $L/\mathbb{Q}$ is Galois if and only if $\#\operatorname{Aut}_{L/\mathbb{Q}} = 2m$. We certainly know that $\#\operatorname{Aut}_{L/\mathbb{Q}} \geq m$ because L/K is Galois and $\#\operatorname{Aut}_{L/K} = m$. If $\tau(L) = L$ then $\tau \in \operatorname{Aut}_{L/\mathbb{Q}}$. However, $\tau \notin \operatorname{Aut}_{L/K}$ because τ does not fix K. Hence, under the assumption that $\tau(L) = L$ we know that $\#\operatorname{Aut}_{L/\mathbb{Q}} \geq m + 1$ and since $\#\operatorname{Aut}_{L/\mathbb{Q}} | 2m$ we conclude $\#\operatorname{Aut}_{L/\mathbb{Q}} = 2m$.

Thus, to show L is Galois over $\mathbb{Q}$ it suffices to prove that $\tau(L) = L$. Let $\mathfrak{m}$ be the modulus $f\mathcal{O}_K$. By Theorem 5 and Example 1 we know that $\ker\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}} = P_K(f)$ and therefore

$$\ker\left(\left(\frac{\tau(L)/K}{\cdot}\right)_{\mathfrak{m}}\right) = \tau\left(\ker\left(\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}\right)\right) = \tau(P_K(f)) = P_K(f) = \ker\left(\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}\right),$$

where the first equality follows easily from the definition of the Artin symbol (1). Since

$$\ker\left(\left(\frac{\tau(L)/K}{\cdot}\right)_{\mathfrak{m}}\right) = \ker\left(\left(\frac{L/K}{\cdot}\right)_{\mathfrak{m}}\right),$$

the equality $\tau(L) = L$ is now an easy consequence of Corollary 6. □

We can now prove the main theorem of this paper:

Proof of Theorem 7. Let L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$. By Lemma 9 we know that $L/\mathbb{Q}$ is Galois. We claim that at least one of the primitive elements that generates L/K is a real algebraic integer. Indeed, begin by noting $L \cap \mathbb{R}$ is the fixed field of L under complex conjugation (an automorphism of order 2). Hence

$$[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]. \tag{3}$$

Let α be an element such that $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$. Then $L = K(\alpha)$. Indeed, it follows from (3) that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq [K(\alpha) : K]$. But

$$[K(\alpha) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K(\alpha) : K] \cdot [K : \mathbb{Q}] \tag{4}$$

$$\implies \frac{[K(\alpha) : \mathbb{Q}(\alpha)]}{2} = \frac{[K(\alpha) : K]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \leq 1. \tag{5}$$

Hence $[K(\alpha) : \mathbb{Q}(\alpha)] = 1$ or 2. But α is real and K is quadratic imaginary, so $[K(\alpha) : \mathbb{Q}(\alpha)] = 2$. From (5) we deduce that $[L : K] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K(\alpha) : K]$, whence $L = K(\alpha)$.

Now take $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ such that $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$. Then $L = K(\alpha)$ by the above remarks. Let $f_n(X) \in \mathbb{Z}[X]$ be the minimal polynomial for this α over K. Since the discriminant of $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ is $-4n$ it follows that

$$\deg f_n(X) = [L : K] = h(\mathcal{O}) = h(-4n)$$

where the second equality holds because L is the ring class field for $\mathcal{O}$. Recall that, by Theorem 8, $p = x^2 + ny^2$ if and only if p splits completely in L. Thus, we want to show that

$$p \text{ splits completely in } L \iff \begin{cases} \left(\dfrac{-n}{p}\right) = 1 \text{ and } f_n(X) \equiv 0 \bmod p \\ \text{has a solution for some } x \in \mathbb{Z}. \end{cases} \tag{6}$$

If p splits completely in L then it splits completely in K (this is due to the transitivity of inertial degrees and ramification indices). It is a well-known fact in algebraic number theory that a rational p splits in a quadratic imaginary field if and only if the discriminant of the field is a square modulo p and so $\left(\dfrac{-n}{p}\right) = 1$. Let $K = \mathbb{Q}(\sqrt{-n})$; then $d_K = -n$ or $-4n$. In either case we conclude that

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}} \iff \left(\frac{-n}{p}\right) = 1.$$

Since $p \nmid \operatorname{disc} f_n(X)$ by hypothesis we know that $f_n(X)$ is separable over F_p. But p splits completely in K, which means $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, and so $f_n(X)$ is separable over $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. Hence

$$\mathfrak{p} \text{ splits completely in } L \iff f_n(X) \equiv 0 \bmod \mathfrak{p} \text{ has a solution in } \mathcal{O}_K$$

(this is a standard result; see [Mar, Theorem 27]). Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$ we have

$$f_n(X) \equiv 0 \bmod \mathfrak{p} \text{ has a solution in } \mathcal{O}_K \iff f_n(X) \equiv 0 \bmod p \text{ has a solution in } \mathbb{Z}.$$

Thus

$$p \text{ splits completely in } L \implies \begin{cases} \left(\dfrac{-n}{p}\right) = 1 \text{ and } f_n(X) \equiv 0 \bmod p \\ \text{has a solution for some } x \in \mathbb{Z}. \end{cases}$$

For the other direction, note that if $f_n(X) \equiv 0 \bmod p$ has a solution in $\mathbb{Z}$ then $f_n(X) \equiv 0 \bmod \mathfrak{p}$ has a solution in $\mathcal{O}_K$ and so $\mathfrak{p}$ splits completely in L. We know p splits completely in K and so by an argument similar to that at the end of the proof to Theorem 8 we conclude p splits in L, as desired. □

4 When is $p = x^2 + ny^2$?

Recall that Theorem 7 does not explicitly give the polynomial $f_n(X)$ which can be used to determine when $p = x^2 + ny^2$; it merely asserts that the polynomial exists. In this section we give a method for computing $f_n(X)$[1].

[1]This section is rather concise since I did much of this for my thesis. The bulk of what I learned for this project is in §2 and 3.

Let L be a lattice and define the quantities

$$g_2(L) = 60 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad g_3(L) = 140 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^6}$$

These sums are absolutely convergent. We define the j-invariant of a lattice by

$$j(L) = \frac{1728 g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2}.$$

This quantity is always defined as one can show that $\Delta(L) := g_2(L)^3 - 27 g_3(L)^2$ does not vanish. The j-invariant of a lattice characterizes the lattice up to homothety. If the lattice L is of the form $[1, \tau]$ for some τ with positive imaginary part then we write $j(\tau)$ instead of $j(L)$.

Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$. These numbers are linearly independent over $\mathbb{R}$ since K is imaginary quadratic and thus $\mathfrak{a}$ gives rise to a lattice. We denote its j-invariant by $j(\alpha)$.

The first main theorem of complex multiplication asserts that $j(\mathfrak{a})$ is a primitive element for the ring class field of the order $\mathcal{O}$ (see [Cox, Theorem 11.1]).

Theorem 10. *Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order in K. Suppose $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field for the order $\mathcal{O}$.*

In particular, we consider the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in the ring $K = \mathbb{Q}[\sqrt{-n}]$. If we can show that $j(\sqrt{-n})$ is a real number, then Theorem 10 reduces the search for the polynomial $f_n(X)$ of Theorem 7 to the computation of the minimal polynomial for $j(\sqrt{-n})$.

Theorem 11. *The algebraic integer $j(\sqrt{-n})$ is a real number.*

Proof. Let $\overline{L}$ denote the conjugate lattice to L. It is clear that

$$g_2(\overline{L}) = \overline{g_2(L)} \quad \text{and} \quad g_3(\overline{L}) = \overline{g_3(L)},$$

and therefore $j(\overline{L}) = \overline{j(L)}$. Now, $j(L)$ is real if and only if $j(L) = \overline{j(L)}$, and by the previous remarks this happens if and only if $j(L) = j(\overline{L})$. Since the j-invariant of a lattice classifies the lattice up to homothety, we conclude $j(L)$ is real if and only if L and $\overline{L}$ are homothetic lattices. This is clear when $L = [1, \sqrt{-n}]$. Hence $j(\sqrt{-n})$ is real, as desired. □

It remains to compute the minimal polynomial $H_{-4n}(X)$ for $j(\sqrt{-n})$. Then we will have a criterion that tells us when $p = x^2 + ny^2$ for primes that don't divide $-4n$ or $\operatorname{disc} H_{-4n}(X)$[2]. It turns out that

$$H_{-4n}(X) = \prod_{i=1}^{h(-4n)} (X - j(\mathfrak{a}_i))$$

[2]It turns out that if $p | \operatorname{disc} H_{-4n}(X)$ then $\left(\frac{-n}{p}\right) \neq 1$—see [Cox, Corollary 13.22]; that is, the condition $p \nmid \operatorname{disc} H_{-4n}(X)$ is superfluous.

as $\mathfrak{a}_i$ ranges through a representative system of ideal classes in $C(\mathcal{O})$. See, for example, [Cox, Proposition 13.2].

4.1 An example: $p = x^2 + 21y^2$

We now show a simple example of how one can implement the algorithm presented in Theorem 7. We consider the case when $n = 21$. In this case the order $\mathbb{Z}[\sqrt{-21}]$ is the maximal order of $K = \mathbb{Q}(\sqrt{-21})$.One may check that the ideal class group of this field is the Klein group. Explicitly,

$$C(\mathcal{O}_K) = \{[\mathcal{O}_K], [P_2], [P_3], [P_5]\},$$

where

$$\begin{aligned} P_2 &= (2, \sqrt{-21} - 1), \\ P_3 &= (3, \sqrt{-21}), \\ P_5 &= (5, \sqrt{-21} - 3), \end{aligned}$$

and the relations $[P_2]^2 = [\mathcal{O}_K]$, $[P_3]^2 = [\mathcal{O}_K]$ and $[P_5] = [P_2] \cdot [P_3]$ hold.

With the aid of the widely available PARI-GP software (which uses the method of q-expansions to compute j-invariants), we compute the approximations

$$\begin{aligned} j(\sqrt{-21}) &= 3196802718613.9132928032899986... \\ j\left(\frac{\sqrt{-21}-1}{2}\right) &= -1787216.6012476570198674... \\ j\left(\frac{\sqrt{-21}}{3}\right) &= 15488.6808931242445923... \\ j\left(\frac{\sqrt{-21}-3}{5}\right) &= 58.0070617294852765... \end{aligned}$$

Using the above approximations for the elements of J, we conjecture, with some margin of error, that the irreducible polynomial for $j(\mathcal{O}_K)$ is

$$\begin{aligned} P(X) = x^4 &- 3196800946944x^3 - 566367922308530952x^2 \\ &+ 888212465898100893941 76x - 513320165321098605782 6304 \end{aligned}$$

To see whether a prime p can be written in the form $x^2 + ny^2$ we need only check that $\left(\frac{-21}{p}\right) = 1$ and that $P(X)$ has a solution over $\mathbb{F}_p$. This last step is easily done with computer power.

References

[Cox] Cox, D. A. *Primes of the form $x^2 + ny^2$* John Wiley & Sons, New York, 1989.

[F–T] Fröhlich, A. & Taylor, M. J. *Algebraic Number Theory* Cambridge University Press, Cambridge, 1991.

[Ked] K. S. Kedlaya, *Complex Multiplication and Explicit Class Field Theory*, Senior Honors Thesis, Harvard University, 1996.

[Lang] Lang, S. *Algebraic Number Theory* Springer, New York, 1986.

[Mar] Marcus, D. A. *Number Fields* Springer, New York, 1977.

[Neu] Neukirch, J. *Class Field Theory* Grund. der Math. Wiss. 280 Springer, Berlin, 1986.

[Sil 2] Silverman, J. *Advanced Topics in the Arithmetic of Elliptic Curves* Springer, New York, 1994.