INTRODUCTION TO CLASS FIELD THEORY

BOWEN WANG

Abstract. This paper introduces basic theorems of class field theory and discusses Hilbert class fields. As an application of Hilbert class field, a partial solution to the problem "primes of the form $p = x^2 + ny^2$" is given.

Contents

1. Theorems of Class Field Theory 1
2. Solution of $p = x^2 + ny^2$ for infinitely many n 7
Appendix A. A Quadratic Field Example 10
Acknowledgments 11
References 11

1. Theorems of Class Field Theory

In this section we will introduce some theorems of class field theory and discuss the Hilbert class field of a number field. In order to discuss class field theory, we first define the unramified extension:

Definition 1.1. Prime ideals of $\mathcal{O}_K$ are called *finite primes* to distinguish them from *infinite primes*, which are embeddings of K into $\mathbb{C}$. A real infinite prime is an embedding $\sigma : K \longrightarrow \mathbb{R}$, while a complex infinite prime is a pair of complex conjugate embeddings $\sigma, \bar{\sigma} : K \longrightarrow \mathbb{C}, \sigma \neq \bar{\sigma}$.

Definition 1.2. Let $K \subset L$ be a finite extension. Then, an infinite prime σ of K *ramifies* in L if σ is real but has an extension to L which is complex. An extension $K \subset L$ is *unramified* if it is unramified at all primes, finite or infinite.

Intuitively, the Hilbert class field of a number field K is the maximal unramified extension of K (a formal definition will be given later). However, the existence of Hilbert class fields is nontrivial and we need to develop some class field theory in order to show it.

We first introduce the notion of a modulus, which is important in theorems of class field theory.

Definition 1.3. Given a number field K, a *modulus* in K is a formal product

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

over all primes $\mathfrak{p}$, finite or infinite, of K, where the exponents must satisfy:

(i) $n_{\mathfrak{p}} \geq 0$, and at most finitely many are nonzero.
(ii) $n_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is a complex infinite prime.

(iii) $n_{\mathfrak{p}} \leq 1$ if $\mathfrak{p}$ is a real infinite prime.

A modulus $\mathfrak{m}$ may thus be written as $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. When all of the exponents $n_{\mathfrak{p}} = 0$, we set $\mathfrak{m} = 1$. Note that for a purely imaginary field K, a modulus is simply an ideal of $\mathcal{O}_K$.

We can now generalize the idea of ideal class group using the modulus $\mathfrak{m}$.

Definition 1.4. Given a modulus $\mathfrak{m}$, let $I_K(\mathfrak{m})$ be the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}$, and let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies

$$\alpha \equiv 1 \bmod \mathfrak{m} \text{ and } \sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma \text{ dividing } \mathfrak{m}_\infty$$

Definition 1.5. A subgroup $H \subset I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if it satisfies

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

and the quotient $I_K(\mathfrak{m})/H$ is called a *generalized ideal class group* for $\mathfrak{m}$.

Notice that if we take $\mathfrak{m} = 1$, then $P_K = P_{K,1}(1)$ is a congruence subgroup. Therefore the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ is a generalized ideal class group. The main idea of class field theory, as we shall see, is the correspondence between the generalized ideal class group and the Galois group of abelian extensions of K, which are linked via the Artin map. Therefore we will now discuss the Artin symbol and the Artin map to see the isomorphism which defines the Hilbert class field.

Lemma 1.6. *Let $K \subset L$ be a Galois extension, and let P be a prime of $\mathcal{O}_K$ which is unramified in L. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing P, then there is a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

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

where $N(P) = |\mathcal{O}_K/P|$ is the norm of P.

Proof. Let $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ be the decomposition and inertia groups of $\mathfrak{P}$, respectively. Recall that $\sigma \in D_{\mathfrak{P}}$ induces an element $\tilde{\sigma} \in \tilde{G}$, where $\tilde{G}$ denotes the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/P$. Since P is unramified in L, it follows that $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|P} = 1$, and then we have $D_{\mathfrak{P}} \cong \tilde{G}$ since $I_{\mathfrak{P}}$ is the kernel of the surjective homomorphism. It is clear that if $\mathcal{O}_K/P$ has q elements, then $\tilde{G}$ is a cyclic group with generator being the Frobenius map $x \mapsto x^q$. Thus there is a unique $\sigma \in D_{\mathfrak{P}}$ which maps to the Frobenius map. Since $q = N(p)$ by definition, σ satisfies the desired condition

$$\sigma(\alpha) \equiv \alpha^{N(P)} \bmod \mathfrak{P} \ \forall \alpha \in \mathcal{O}_L.$$

The uniqueness follows easily from the fact that any σ satisfying this condition must lie in $D_{\mathfrak{P}}$. □

Definition 1.7. The unique element σ in lemma 1.6 is called the *Artin symbol* and is denoted by $((L/K)/\mathfrak{P})$.

The Artin symbol has the following useful properties:

Corollary 1.8. *Let $K \subset L$ be a Galois extension, and let P be an unramified prime of K. Given a prime $\mathfrak{P}$ of L containing P, we have:*

(i) If $\sigma \in \mathrm{Gal}(L/K)$, then

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

(ii) The order of $((L/K)/\mathfrak{P})$ is the inertial degree $f = f_{\mathfrak{P}|P}$.
(iii) P splits completely in L if and only if $((L/K)/\mathfrak{P}) = 1$.

Proof. For (i), notice that

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) \equiv \sigma((\sigma^{-1}(\alpha))^{N(\mathfrak{P})}) \equiv \alpha^{N(\mathfrak{P})} \bmod \mathfrak{P}$$

However,

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)(\alpha) \equiv \alpha^{N(\sigma(\mathfrak{P}))} \bmod \mathfrak{P}$$

and $N(\mathfrak{P}) = N(\sigma(\mathfrak{P}))$. Therefore, the uniqueness of Artin symbol shows that

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

For (ii), since P is unramified, the decomposition group is isomorphic to the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/P$ whose degree is the inertial degree f. Since the Artin symbol maps to a generator of the Galois group, it follows that the Artin symbol has order f.

For (iii), notice that P splits completely in L if and only if $e = f = 1$. Since we have already assumed that $e = 1$, (iii) follows trivially from (ii). □

When $K \subset L$ is an abelian extension, the Artin symbol $((L/K)/\mathfrak{P})$ depends only on the underlying prime $P = \mathfrak{P} \cap \mathcal{O}_K$. To see this, let $\mathfrak{P}'$ be another prime containing P. Notice that $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in \mathrm{Gal}(L/K)$. Then corollary 1.8 implies that

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

since $\mathrm{Gal}(L/K)$ is abelian. It follows that whenever $K \subset L$ is abelian, the Artin symbol can be written as $((L/K)/P)$.

As an example of the use of the Artin symbol, we can prove quadratic reciprocity without much effort:

Lemma 1.9. *The cyclotomic extension $\mathbb{Q}(\zeta_n)$ is an abelian extension of $\mathbb{Q}$. In fact, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Proof. This is a standard result on cyclotomic fields. For a proof, see [5]. □

Theorem 1.10. *If p, q be distinct odd primes in $\mathbb{Z}$, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. Consider the cyclotomic extension $Q \subset \mathbb{Q}(\zeta_p)$. If $q \neq p$, then $x^p - 1$ is separable modulo q since $\gcd(x^p - 1, px^{p-1}) = 1$. Therefore, q is unramified in $\mathbb{Q}(\zeta_p)$. Moreover, $1, \zeta, \ldots, \zeta^{p-1}$ are distinct modulo q. But by the definition of the Artin symbol,

$$\left(\frac{(\mathbb{Q}(\zeta_p)/\mathbb{Q})}{q}\right)(\zeta) \equiv \zeta^{N(q)} \equiv \zeta^q \bmod q.$$

Hence by the uniqueness of the Artin symbol, $((\mathbb{Q}(\zeta_p)/\mathbb{Q})/q)$ is the map $\zeta \mapsto \zeta^q$.

Notice that $(q/p) \equiv q^{\frac{p-1}{2}} \bmod p$ by Euler's criterion. Therefore, q is a square mod p if and only if q is in the subgroup of order $\frac{p-1}{2}$ of $(\mathbb{Z}/p\mathbb{Z})^*$. But then the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ tells us that $((\mathbb{Q}(\zeta_p)/\mathbb{Q})/q)$ fixes the unique quadratic subextension $K' = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$ squarefree. But since p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$, it follows that p ramifies in K', which means that $m = (-1)^{\frac{p-1}{2}} p$. Therefore, $((K'/\mathbb{Q})/q) = 1$ and therefore q splits completely in K'. This implies that

$$x^2 - (-1)^{\frac{p-1}{2}} p \equiv 0 \bmod q$$

has solution in $\mathbb{Z}$, which means that

$$\left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = \left(\frac{q}{p}\right).$$

□

Now we define the Artin map in terms of the Artin symbol:

Definition 1.11. Let $\mathfrak{m}$ be a modulus divisible by all ramified primes of an abelian extension $K \subset L$. Given a prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, we have the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$$

and it extends by multiplicativity to give a homomorphism

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

which is called the *Artin map* for $K \subset L$. When we want to refer explicitly to the extension involved, we will write $\Phi_{L/K,\mathfrak{m}}$ instead of $\Phi_{\mathfrak{m}}$.

Now in order to see the correspondence between generalized ideal class groups and Galois groups of abelian extensions, we need the following three important theorems of class field theory. The proofs can be found in Janusz's book [4].

Theorem 1.12 (Artin Reciprocity Theorem)**.** *Let $K \subset L$ be an abelian extension, and let $\mathfrak{m}$ be a modulus divisible by all primes of K, finite or infinite, that ramifies in L. Then:*

(i) The Artin map $\Phi_{\mathfrak{m}}$ is surjective.

(ii) If the exponents of the finite primes dividing $\mathfrak{m}$ are sufficiently large, then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, i.e.,

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \subset I_K(\mathfrak{m})$$

and consequently the isomorphism

$$I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \simeq \mathrm{Gal}(L/K)$$

shows that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for the modulus $\mathfrak{m}$.

Theorem 1.13 (Conductor Theorem)**.** *Let $K \subset L$ be an abelian extension. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that*

(i) A prime of K, finite or infinite, ramifies in L if and only if it divides $\mathfrak{f}$.

(ii) Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f} \mid \mathfrak{m}$.

The modulus $\mathfrak{f}(L/K)$ is uniquely determined by $K \subset L$ and is called the *conductor* of the extension.

Theorem 1.14 (Existence Theorem)**.** *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$, i.e,*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Then there is a unique abelian extension L of K with all its ramified primes, finite or infinite, dividing $\mathfrak{m}$ such that if

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

is the Artin map of $K \subset L$, then

$$H = \ker(\Phi_{\mathfrak{m}}).$$

We have the following corollary from the three theorems we just stated:

Corollary 1.15. *Let L and M be Abelian extensions of K. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all primes of K ramified in either L or M, such that*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}}).$$

Proof. We first prove the following lemma:

Lemma 1.16. *Let $K \subset L$ be an abelian extension, and let $\mathfrak{m}$ be a modulus for which the Artin map $\Phi_{\mathfrak{m}}$ is defined. If $\mathfrak{n}$ is another modulus and $\mathfrak{m} \mid \mathfrak{n}$, then*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \implies P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).$$

Proof. Given $\alpha\mathcal{O}_K \in P_{K,1}(\mathfrak{n})$, we have $\alpha \equiv 1 \bmod \mathfrak{n}_0$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{n}_\infty$. Since $\mathfrak{m} \mid \mathfrak{n}$, it follows that $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{m}_\infty$. But then by the definition of the Artin symbol

$$\Phi_{\mathfrak{n}}(\alpha\mathcal{O}_K) = \Phi_{\mathfrak{m}}(\alpha\mathcal{O}_K) = 1_{\mathrm{Gal}(L/K)}.$$

Therefore,

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \implies P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).$$

□

Now first assume $L \subset M$, and let $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ be the restriction map. By the Artin reciprocity theorem and lemma 1.16, there is a modulus $\mathfrak{m}$ for which $\Phi_{L/K,\mathfrak{m}}$ and $\Phi_{M/K,\mathfrak{m}}$ are both congruence subgroups for $\mathfrak{m}$. Then by the uniqueness of Artin symbol, $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$, and then it is clear that $\ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$.

For the other direction, assume that $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$. Then under the map $\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$, the subgroup $\ker(\Phi_{L/K,\mathfrak{m}})$ is mapped to a subgroup $H \subset \mathrm{Gal}(M/K)$. By Galois theory, H corresponds to an intermediate field $K \subset \tilde{L} \subset M$. Then the first part of the proof shows that

$$\ker(\Phi_{\tilde{L}/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}}).$$

Then the uniqueness part of the existence theorem implies that $L = \tilde{L} \subset M$. Hence the corollary is proved. □

As a simple corollary, we can prove Kronecker-Weber theorem :

Theorem 1.17 (Kronecker-Weber)**.** *Let L be an abelian extension of $\mathbb{Q}$. Then there is a positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$, where ζ_m is the mth root of unity.*

Proof. By Artin Reciprocity theorem, there is a modulus $\mathfrak{m}$ such that $P_{\mathbb{Q},1}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q}}, \mathfrak{m})$, and by lemma 1.14, we may assume that $\mathfrak{m} = m\infty$, where ∞ is the real infinite prime of $\mathbb{Q}$. Notice that any prime not dividing m is unramified in $\mathbb{Q}(\zeta_m)$, and it follows that the Artin map

$$\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

is defined. $\Phi_{\mathfrak{m}}$ can be described as follows: given $(a/b)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$, where $(a/b) > 0$ and $\gcd(a, m) = \gcd(b, m) = 1$, then

$$\Phi_{\mathfrak{m}}(\frac{a}{b}\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Therefore,

$$\ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}}).$$

Hence by corollary 1.13 we conclude that $L \subset \mathbb{Q}(\zeta_m)$. □

Next, we shall formally discuss the Hilbert class field. If we apply the Existence Theorem to the modulus $\mathfrak{m} = 1$ and the subgroup $P_K \subset I_K$, there is a unique abelian extension L of K, unramified since $\mathfrak{m} = 1$, such that the Artin map induces an isomorphism

$$\mathrm{Cl}(\mathcal{O}_K) = I_K/P_K \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

L is defined to be the *Hilbert class field* of K, and has the following property:

Theorem 1.18. *The Hilbert class field L is the maximal unramified abelian extension of K.*

Proof. Let M be an unramifed abelian extension. The first part of the Conductor theorem implies that $\mathfrak{f}(M/K) = 1$ since a prime ramifies if and only if it divides the conductor. Then the second part shows that $\ker(\Phi_{M/K,1})$ is a congruence subgroup for the modulus 1, which means

$$P_K \subset \ker(\Phi_{M/K,1}).$$

By the definition of the Hilbert class field, this shows that

$$P_K = \ker(\Phi_{L/K,1}) \subset \ker(\Phi_{M/K,1})$$

and $M \subset L$ follows from corollary 1.13. □

We then have the following corollary which characterizes all primes that split completely in the Hilbert class field:

Corollary 1.19. *Let L be the Hilbert class field of a number field K, and let P be a prime ideal of K. Then P splits completely in L if and only if P is a principal ideal.*

Proof. By corollary 1.8, we know that P splits completely if and only if $((L/K)/P) = 1$. Since the Artin map induces an isomorphism $\mathrm{Cl}(\mathcal{O}_K) \cong \mathrm{Gal}(L/K)$, it is clear that $((L/K)/P) = 1$ if and only if P determines the trivial class of $\mathrm{Cl}(\mathcal{O}_K)$. Thus by definition, P is principal. □

The power of the Hilbert class field will soon become clear as we shall see an application in the next section.

2. Solution of $p = x^2 + ny^2$ for infinitely many n

In this section we will apply the theorems from the previous section on Hilbert class field to give a partial solution to the problem $p = x^2 + ny^2$ where p is prime.

We first state the main theorem, which gives solution of $p = x^2+ny^2$ for infinitely many n:

Theorem 2.1. *Let $n > 0$ be an integer satisfying the following condition:*

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

Let $h(-4n)$ denote the order of the ideal class group of the quadratic field with discriminant $-4n$. 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

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

The proof of the theorem is built on several nontrivial results:

Theorem 2.2. *Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{n})$. Assume that n is squarefree and that $n \not\equiv 3 \bmod 4$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. If p is an odd prime not dividing n, then*

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

Proof. Suppose that n is squarefree and that $n \not\equiv 3 \bmod 4$. Then it follows that $d_K = -4n$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Suppose p is an odd prime not dividing n, Then $p \nmid d_K$, which means p is unramified in K. We shall prove the following equivalences:

$$\begin{aligned} p = x^2 + ny^2 &\iff p\mathcal{O}_K = P\bar{P}, \text{and } P \text{ is principal in } \mathcal{O}_K \\ &\iff p\mathcal{O}_K = P\bar{P}, P \neq \bar{P}, \text{and } P \text{ splits completely in } L \\ &\iff p \text{ splits completely in } L \end{aligned} \tag{2.3}$$

To prove the first equivalence, suppose that

$$p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y).$$

Let $P = (x + \sqrt{-n}y)\mathcal{O}_K$, then $p\mathcal{O}_K = P\bar{P}$ must be the prime factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$. Note that $P \neq \bar{P}$ since p is unramified in K. Conversely, suppose that

$$p\mathcal{O}_K = P\bar{P},$$

where P is principal. Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$, we can write $P = (x+\sqrt{-n}y)\mathcal{O}_K$. This implies that $p\mathcal{O}_K = (x^2 + ny^2)\mathcal{O}_K$, which means that $p = x^2 + ny^2$.

The second equivalence follows immediately from corollary 1.19. To prove the final equivalence, we shall need some lemmas:

Lemma 2.4. *Let K be an imaginary quadratic field, and let $K \subset L$ be a Galois extension and let τ be complex conjugation. Then L is Galois over $\mathbb{Q}$ if and only if $\tau(L) = L$.*

Proof. Let $M \supset L$ be a Galois extension of $\mathbb{Q}$ that contains L. Let A and B denote the subgroup of $G = \mathrm{Gal}(M/\mathbb{Q})$ that fixes K and L respectively. Then since $K = \mathbb{Q}(\sqrt{-n})$ for some n, it follows that $G/B = \{1, \tau\}$. Notice that since L/K is Galois, it follows that A is a normal subgroup of B. Then we want to show

that A is normal in G if and only if $\tau A = A\tau$. But since every element of G can be written as b or τb for some $b \in B$, and A is normal in B, it follows that A is normal in $G \iff \tau A = A\tau$. □

Lemma 2.5. *Let L be the Hilbert class field of an imaginary quadratic field K, and let τ denote complex conjugation. Then $\tau(L) = L$, and therefore L is Galois over $\mathbb{Q}$.*

Proof. It is easy to see that $\tau(L)$ is an unramified abelian extension of $\tau(K) = K$. Since L is the maximal such extension, we have $\tau(L) \subset L$, and therefore $\tau(L) = L$ since they have the same degree over K. Hence $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, which implies that L is Galois over $\mathbb{Q}$ by lemma 2.4.

□

Lemma 2.6. *If $K \subset M \subset L$ are number fields where L and M are Galois over K, then a prime p of $\mathcal{O}_K$ splits completely in L if and only if it splits completely in M and some prime of $\mathcal{O}_M$ containing p splits completely in L.*

Proof. Suppose p splits completely in L; then the lemma follows from the multiplication property of ramification index and inertial degree on towers.

Conversely, let $P \subset \mathcal{O}_M$ be a prime containing p. Then we know that $P = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ in $\mathcal{O}_L$ where $n = [L : M]$. But then $\mathfrak{P}_i$ appear in the prime factorization of p in $\mathcal{O}_L$. Since L is Galois over K, it follows that all the ramification indices and inertial degrees of p are the same, which means they are all 1 by tower law. Therefore, p splits completely in L. □

Now notice that the condition

$$p\mathcal{O}_K = P\bar{P}, P \neq \bar{P}, \text{ and } P \text{ splits completely in } L.$$

says that P splits completely in K and that some prime of K containing p splits completely in L. Since L is Galois over $\mathbb{Q}$, this implies that p splits completely in L by lemma 2.6. □

The next step is to give a more elementary way of saying that p splits completely in L. We have the following criterion:

Proposition 2.7. *Let K be an imaginary quadratic field, and let L be a finite extension of K which is Galois over $\mathbb{Q}$. Then:*

(i) There is a real algebraic integer α such that $L = K(\alpha)$.
(ii) Let α be as in (i), let $f(x) \in \mathbb{Z}[x]$ denote its minimal polynomial. If p is a prime not dividing the discriminant of $f(x)$, then

$$p \text{ splits completely in } L \iff \begin{cases} (d_K/p) = 1 \text{ and } f(x) \equiv 0 \bmod p \\ \text{has an integer solution} \end{cases}$$

Proof. For (i), we need the following lemma:

Lemma 2.8. *Let $K \subset L$ be a finite extension and L is Galois over $\mathbb{Q}$, then*

(a) $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$
(b) For $\alpha \in L \cap \mathbb{R}, L \cap \mathbb{R} = \mathbb{Q}(\alpha) \iff L = K(\alpha)$.

Proof. Notice that since $L \cap \mathbb{R}$ is the fixed field of complex conjugation, by lemma 2.4 we have $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$. Now let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Then we shall prove that f is irreducible over K. Suppose $f(x) = p_1(x) \cdots p_n(x)$ where $p_i(x)$ are irreducible polynomials in $K[x]$ and $n \geq 2$. Now since f splits in L, we know that $p_i(\alpha) = 0$ for some i. Without loss of generality, suppose α is a root of $p_1(x)$. Now consider the splitting field $M \supset K$ of $p_1(x)$. It then follows that $M = K(\alpha)$ since M is Galois over K and α is a root of $p_1(x)$. Now since α is real, it follows that $\tau(M) = M$ where τ is complex conjugation. Therefore by lemma 2.4 we know that M is Galois over $\mathbb{Q}$. It then follows that f splits in M, which implies $[M : Q] \geq \deg(f)) = [L \cap \mathbb{R} : \mathbb{Q}]$. But since $M \subset L$ and $[L : L \cap \mathbb{R}] = [K : \mathbb{Q}]$, it follows that $M = L$ because $M \neq L \cap \mathbb{R}$. But then $[L : K] = \deg(p_1) < \deg(f) = [L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$, which is a contradiction. Therefore f is irreducible over K. Thus by the same argument as above, we see that $L = K(\alpha)$. The converse can be similarly proved. □

Hence, if $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ satisfies $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$, then it follows that $L = K(\alpha)$ and (i) is proved.

To prove (ii), let p be a prime not dividing the discriminant of $f(x)$. This implies that $f(x)$ is separable modulo p. But by ramification theory of quadratic field, we have

$$p\mathcal{O}_K = P\bar{P}, P \neq \bar{P} \iff \left(\frac{d_K}{p}\right) = 1.$$

We may assume that p splits completely in K since both side implies this condition. Therefore $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/P$. Since $f(x)$ is separable over $\mathbb{Z}/p\mathbb{Z}$, it is separable over $\mathcal{O}_K/P$, and then we have

$$\begin{aligned} P \text{ splits completely in } L &\iff f(x) \equiv 0 \bmod P \text{ is solvable in } \mathcal{O}_K \\ &\iff f(x) \equiv 0 \bmod p \text{ is solvable in } \mathbb{Z} \end{aligned}$$

Then the proposition follows from the last equivalence of (2.3) . □

We can now prove theorem 2.1:

Proof. Since the Hilbert class field L of $K = \mathbb{Q}(\sqrt{-n})$ is Galois over $\mathbb{Q}$, proposition 2.7 shows that there is a real algebraic integer α which is a primitive element of L over K. Let $f_n(x)$ be the monic minimal polynomial of α, and let p be an odd prime dividing neither n nor the discriminant of $f_n(x)$, then theorem (2.2) and proposition (2.7) imply that

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

It remains to show that the degree of $f_n(x)$ is the class number of $h(-4n)$. By definition of Hilbert class field, we know that $f_n(x)$ has degree

$$[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Cl}(\mathcal{O}_K)| = h(-4n),$$

which completes the proof of theorem 2.1. □

Warning 2.9. The polynomial $f_n(x)$ in theorem 2.1 is *not* unique.

Appendix A. A Quadratic Field Example

Note that theorem 2.1 does not give us an explicit formula for computing $f_n(x)$. In fact, it is usually hard to work out $f_n(x)$ explicitly, but for certain quadratic fields, we can compute $f_n(x)$ explicitly by computing its Hilbert class field:

Proposition A.1. *The Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$ is $L = K(\alpha)$ where $\alpha = \sqrt{\frac{1+\sqrt{17}}{2}}$.*

Proof. First note that $h(-68) = 4$. Therefore, the Hilbert class field has degree 4 over K. Then $L = K(\alpha)$ will be the Hilbert class field once we show that $K \subset L$ is an unramified abelian extension of degree 4. It is easy to show that $K \subset L$ is abelian of degree 4, so we only need to show that it is unramified. Moreover, since K is an imaginary quadratic field, the infinite primes are automatically unramified.

Notice that $\alpha^2 = (1+\sqrt{17})/2$, which means $\sqrt{17} \in L$. If we take $K_1 = K(\sqrt{17})$, then we have the extension

$$K \subset K_1 \subset L$$

and it suffices to show that $K \subset K_1$ and $K_1 \subset L$ are unramified extensions. We need the following lemma:

Lemma A.2. *Let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathcal{O}_K$, and let P be prime in $\mathcal{O}_K$. Then:*

(i) If $2u \notin P$, then P is unramified in L.
(ii) If $2 \in P, u \notin P$ and $u = b^2 - 4c$ for some $b, c \in \mathcal{O}_K$, then P is unramified in L.

Proof. For (i), since the discriminant of $x^2 - u$ is $4u \notin P$, $x^2 - u$ is separable modulo P. Therefore P is unramified in L.

For (ii), notice that $L = K(\beta)$, where $\beta = (-b + \sqrt{u})/2$ is a root of $x^2 + bx + c$. The discriminant is $b^2 - 4c = u \notin P$, so P is unramified in L. □

Now let P be a prime in $\mathcal{O}_K$. Since $K_1 = K(\sqrt{17})$, if $2 \notin P$ and $17 \notin P$, then P is unramified by (i). If $2 \notin P$ and $17 \in P$, it follows that no other integer could be in P, as otherwise we would have either $1 \in P$ or $2 \in P$. Therefore $P = (\sqrt{-17})$, which is unramified in K_1. If $2 \in P$, since $17 = 1^2 - 4 \times (-4)$, P is unramified by (ii).

Then we consider the extension $K_1 \subset L$. Let $u = \frac{1+\sqrt{17}}{2}$ and $u' = \frac{1-\sqrt{17}}{2}$. Then since $uu' = -8 \in K_1$, it follows that $\sqrt{u'} \in L$. Therefore, since $\sqrt{u}$ and $\sqrt{u'}$ have the same degree over K_1, we have

$$L = K_1(\sqrt{u}) = K_1(\sqrt{u'})$$

Now let P be a prime in K_1. If $2 \notin P$, then since $u + u' = 1$, either $u \notin P$ or $u' \notin P$, and P is unramified. If $2 \in P$, then since either $u \notin P$ or $u' \notin P$, we may assume $u \notin P$. But u satisfies $x = x^2 - 4$, which means P is unramified by (ii). □

We can now characterize when a prime p is represented by $x^2 + 17y^2$:

Theorem A.3. *If $p \neq 17$ is an odd prime, then*

$$p = x^2 + 17y^2 \iff \begin{cases} (-14/p) = 1 \text{ and } x^4 - 8x^2 - 1 \equiv 0 \bmod 17 \\ \text{has an integer solution} \end{cases}$$

Proof. Since $\alpha = \sqrt{(1+\sqrt{17})/2}$ is a real integral primitive element of the Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$, its minimal polynomial $x^4 - 8x^2 - 1$ can be chosen to be the polynomial $f_{17}(x)$ of theorem 2.1. Its discriminant is $-2^{\cdot}17^2$, so that the only excluded primes are 2 and 17. Then theorem A.3 follows immediately from theorem 2.1. □

Acknowledgments. It is a pleasure to thank my mentors, Yun Cheng and Zhiyuan Ding, for their advice and support thoughrout the program. I would also like to thank Professor Peter May for organizing this wonderful REU.

References

[1] David A. Cox. Primes of The Form $x^2 + ny^2$. John Wiley & Sons, Inc. 1989.
[2] J.S. Milne. Algebraic Number Theory. http://www.jmilne.org/math/CourseNotes/ANT.pdf
[3] Daniel A. Marcus. Number Fields. Springer-Verlag, New York Inc. 1977.
[4] G. Janusz. Algebraic Number Fields. Academic Press, New York. 1977.
[5] Keith Conrad. Cyclotomic Extensions. http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/cyclotomic.pdf