**J.G.I. Noordsij**

# Primes of the form $x^2 + ny^2$

**Bachelor Thesis**

**Thesis Supervisor: Dr. E. Lorenzo Garcia**

**Date Bachelor Examination: June 26, 2015**


**Mathematical Institute, Leiden University**

# Contents

# Introduction

This thesis is concerned with primes which can be represented by the form $x^2 + ny^2$, where $x$, $y$ and $n > 0$ are integers. The main objective will be proving a theorem that, for each positive integer $n$, gives a condition on all but finitely many primes $p$ which is equivalent to the prime $p$ being of the form $x^2 + ny^2$. This will be referred to as the Main Theorem, which is a theorem from the book of Cox, see [Cox13, Thm. 9.2, p. 163].

**Main Theorem.** *Let $n$ be a positive integer. Then there is a polynomial $f_n(x) \in \mathbb{Z}[X]$ which is monic and irreducible and has degree $h(-4n)$, such that, for any odd prime $p$ not dividing $n$ or the discriminant of $f_n(x)$, we have*

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

*Furthermore, a monic integer polynomial $f_n(x)$ of degree $h(-4n)$ satisfies above condition if and only if $f_n(x)$ is irreducible over $\mathbb{Z}$, and is the minimal polynomial of a real algebraic integer $\alpha$, for which we have $L = K(\alpha)$ where, $K = \mathbb{Q}(\sqrt{-n})$ and $L$ is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in $K$.*

For proving this theorem, we use theorems from class field theory. This branch of mathematics describes the relation between abelian extensions of a field, which in our case will be a finite extension of $\mathbb{Q}$, and its generalized ideal class groups. The ideals studied are the ideals of the ring of algebraic integers of such a field, which are the elements whose minimal polynomials over $\mathbb{Q}$ have integer coefficients. Using class field theory, we can define the ring class field as mentioned in the Main Theorem, and show that the primes of the form $x^2 + ny^2$ are exactly the primes that split completely in this ring class field.

The thesis will largely follow the book of Cox, and will be focussed mainly on giving a much more compact proof of the Main Theorem. It will also fill in some parts from Cox's book, which are left as exercises in there. Finally, almost all examples illustrating the results mentioned in the thesis were added, and thus differ from the ones given in the book.

The last part consists of a study of material closely related to the results covered in the previous chapter. This will concern results on the representation of Mersenne primes by the form $x^2 + ny^2$ for specified values of $n$, and the divisibility properties of the integer $x$ in this representation. Finally, there are some results on the representation of Fibonacci and Lucas numbers by this form, and also a conjecture on the identity $L_p = x^2 + py^2$.

## Content of chapters

The first chapter will be an introduction to the problem based on the work of Fermat, who was the first known to mention results of writing primes as the sum of two squares. We will then prove his results with methods similar to those Euler used, by working out special cases of quadratic reciprocity. This will give us results for the case where $n \leq 4$.

The next part will be the work of Legendre, Lagrange and Gauss on quadratic forms. These forms can represent integers and thus also prime numbers. In particular, we will study which prime numbers are represented by the principal form $x^2 + ny^2$. For this, we first study the properties of quadratic forms and introduce an equivalence relation to group them together. Then, we will be able to study these equivalence classes of primitive positive definite forms with discriminant $-4n$, and show that each class represents a certain subset of values in the group $(\mathbb{Z}/4n\mathbb{Z})^*$. Now this can be used to prove our Main Theorem for more values of $n$, but this will still only cover a finite amount of cases.

Chapter 3 will be focused on class field theory, which will give us all the tools needed to prove the Main Theorem. Here some basic algebraic number theory will be introduced, namely the concept of algebraic integers and the behavior of prime ideals in the ring of integers of a number field. Then, we will introduce the Hilbert class field, which can be used to prove the Main Theorem for infinitely many, but not all, values of $n$. Orders will be introduced, which will be the generalization of the ring of integers needed to prove the Main Theorem for all values of $n$. Finally, we will state some reciprocity laws and the Čebotarev density theorem.

In the fourth chapter we will prove the Main Theorem by making use of the results discussed in the third chapter. By defining the ring class field, we can show that a prime $p$ splitting completely in the ring class field is equivalent to the prime being of the form $x^2 + ny^2$. We give a condition, which ensures a prime $p$ splits completely in the field, to complete the proof the Main Theorem. Then, we work out an example of the Main Theorem for the case where $n = 15$, which will show its application.

Finally we will discuss some related results, based on the work of Lenstra and Stevenhagen (see [LJS00]) and Jansen (see [Jan02]) on Mersenne primes of the form $x^2 + dy^2$. We will then study Fibonacci numbers with prime index, which are of the form $4F_p = 5x^2 + py^2$ whenever $p \equiv 3 \bmod 4$ (see [BLM15]). Using the same method, we will prove a similar result for Lucas numbers with prime index. In this representation, given by $4L_p = x^2 + 5py^2$, we study some congruence conditions on $x$ and $y$, by computation of some examples. Finally, there is a conjecture about Lucas primes of the form $L_p = x^2 + py^2$.

## Acknowledgments

I would like to thank my supervisor Elisa for introducing me to this nice subject and her advice on both the book and the related results we have tried to find. Your comments made this thesis a lot more readable than it was originally.

# General notations

We now fix some notation and conventions that will be valid in all chapters.
$n$: a positive integer
$\overline{a} \in (\mathbb{Z}/n\mathbb{Z})$: residue class of $a$ in $(\mathbb{Z}/n\mathbb{Z})$
$\mathbb{Z}[\alpha, \beta]$: the $\mathbb{Z}$-module generated by algebraic integers $\alpha, \beta \in \mathbb{C}$
$[\alpha, \beta]$: the set $\{n\alpha + m\beta \mid n, m \in \mathbb{Z}\}$
$C(D)$: the form class group of forms with discriminant $D$
$h(D)$: the class number of $C(D)$
$\mathcal{O}_K$: the ring of algebraic integers of a number field $K$
$d_K$: the discriminant of a quadratic field $K$
$\mathfrak{a}$: an ideal
$\mathfrak{p}, \mathfrak{P}$: a prime ideal
$N(\alpha)$: the norm of an element $\alpha$
$N(\mathfrak{a})$: the norm of an ideal $\mathfrak{a}$
$\mathcal{O}$: an order in a quadratic field $K$
$I_K, P_K$: the groups of fractional ideals and principal fractional ideals of $\mathcal{O}_K$
$I_K(f)$: the subgroup of $I_K$ generated by the ideals prime to $f$
$P_{K,\mathbb{Z}}(f)$: the subgroup of $P_K$ generated by principal ideals $\alpha\mathcal{O}_K$ with $\alpha \equiv a \bmod f\mathcal{O}_K$ where $\gcd(a, f) = 1$
$I(\mathcal{O}), P(\mathcal{O})$: the groups of fractional ideals and principal fractional ideals of $\mathcal{O}$
$I(\mathcal{O}, f), P(\mathcal{O}, f)$: the subgroups of $I(\mathcal{O})$ and $P(\mathcal{O})$ generated by the ideals prime to $f$
$\mathfrak{m}$: a modulus of a number field $K$
$I_K(\mathfrak{m})$: the subgroup of $I_K$ generated by the ideals prime to $\mathfrak{m}$
$P_{1,\mathbb{Z}}(f)$: the subgroup of $P_K$ generated by principal ideal $\alpha\mathcal{O}_K$ with $\alpha \equiv 1 \bmod f\mathcal{O}_K$
$\Phi_{L/K,\mathfrak{m}}$: the Artin map for the extension $K \subset L$ and modulus $\mathfrak{m}$
$\zeta_K(s)$: the Dirichlet $\zeta$-function of $K$
$A \triangle B$: the difference $(A \setminus B) \cup (B \setminus A)$ of two sets
$\mathcal{P}_K$: the set of all prime ideals of $\mathcal{O}_K$
$\mathcal{S}_{L/K}$: the subset of $\mathcal{P}_K$ of primes that split completely in $L$
$\tilde{\mathcal{S}}_{L/K}$: the subset of $\mathcal{P}_K$ of primes unramified in $L$ with an overlying prime of inertial degree 1
$F_n$: the $n$-th Fibonacci number
$L_n$: the $n$-th Lucas number

# Chapter 1

# Reciprocity

In 1640, Fermat wrote a result in a letter, saying that an odd prime $p$ can be written as a sum of two integer squares if and only if $p$ surpasses by one a multiple of 4, which is now usually denoted by $p \equiv 1 \bmod 4$. Later, he also mentioned similar result where $p$ can be written as $x^2 + 2y^2$ or $x^2 + 3y^2$ where $x$ and $y$ are integers. While he does mention a method of how to prove the statements, no proof by him is known. However, Euler did manage to prove the claims of Fermat, using the method Fermat described. In this section, we will prove the same results, in a way very similar to the work of Euler.

## 1.1 Quadratic reciprocity

For the case where $n \leq 3$, we can give complete proofs of the question whether a prime is of the form $x^2+ny^2$. For this, we will use the methods of Euler, who divided the proof into two parts, named the Reciprocity step and the Descent step. The Reciprocity step will give us a necessary and sufficient condition such that an odd prime $p$ divides a number of the form $x^2 + ny^2$ where $\gcd(x, y) = 1$. Then the Descent step will tell that in case we have that $n \leq 3$, any odd prime $p$ dividing a number of the form $x^2 + ny^2$ will be of the same form. This will yield the result we are aiming for.

We will first consider the Reciprocity step, which is directly linked to the quadratic reciprocity law. We will first define the Legendre symbol.

**Definition 1.1.1.** *(Legendre symbol) Let $a \in \mathbb{Z}$ be an integer and let $p$ be a prime number. We define the* Legendre symbol *as follows*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } \exists x \in \mathbb{Z} : \ a \equiv x^2 \bmod p \\ -1 & \text{if } p \nmid a \text{ and } \nexists x \in \mathbb{Z} : \ a \equiv x^2 \bmod p \end{cases}$$

We can now determine in which cases we have that an odd prime $p$ divides a number of the form $x^2+ny^2$.

**Lemma 1.1.2.** *Let $p$ be an odd prime not dividing $n$. Then we have $p \mid x^2+ny^2$ where $\gcd(x,y)=1$ if and only if $\left(\frac{-n}{p}\right)=1$.*

*Proof.* First suppose we have $p \mid x^2+ny^2$ where $\gcd(x,y)=1$, then we find that $x^2+ny^2 \equiv 0 \bmod p$ and thus

$$-ny^2 \equiv x^2 \bmod p.$$

Since we have $\gcd(x,y)=1$, we find that $y$ is not divisible by $p$. So, we have that $y$ has an inverse $a$ in $(\mathbb{Z}/p\mathbb{Z})^*$, and thus we have $-n \equiv (xa)^2 \bmod p$. Since $p$ and $n$ are coprime, it follows that $\left(\frac{-n}{p}\right)=1$.

Now suppose we have $\left(\frac{-n}{p}\right)=1$, then $-n \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}$. Thus we have $p \mid x^2+n\cdot 1^2$. □

Since we are looking for a congruence condition on primes that ensures a prime can be written as $x^2+ny^2$, we will have to show that, for each value of $n$, there are congruence conditions that ensure that we have $\left(\frac{-n}{p}\right)=1$. This are exactly the classes described in the following theorem.

**Theorem 1.1.3.** *Let $n$ be an integer. Then there exists a unique homomorphism $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \to \{\pm 1\}$ such that, for any odd prime $p$ not dividing $n$, we have*

$$\chi(\bar{p}) = \left(\frac{-n}{p}\right).$$

*Proof.* The result can be proven by making use of the Jacobi symbol, a generalization of the Legendre symbol. Note that uniqueness immediately follows from Dirichlet's theorem on primes in arithmetic progressions (see [IR82, Ch. 16, Thm. 1, p. 251]). □

To compute the residue classes in $\mathbb{Z}/4n\mathbb{Z}$ such that for any odd prime in this class we have that $\left(\frac{-n}{p}\right)=1$, we will use the quadratic reciprocity law and supplementary laws. We will not give a proof of this result, however it can be derived from Theorem 3.4.10.

**Theorem 1.1.4.** *(Quadratic reciprocity law)*

1. *Let $p$ and $q$ be distinct odd prime numbers. Then*

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

2. *Let $p$ be an odd prime number. Then*

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

3. *Let $p$ be an odd prime number. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

By using Theorem 1.1.4, we can now compute for which odd primes $p$ we have that $p$ divides a number of the form $x^2 + ny^2$.

**Corollary 1.1.5.** *(Reciprocity step) Let $p$ be an odd prime. Then we have*

$$p \mid x^2 + y^2 \text{ where } \gcd(x,y) = 1 \iff \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4$$

$$p \mid x^2 + 2y^2 \text{ where } \gcd(x,y) = 1 \iff \left(\frac{-2}{p}\right) = 1 \iff p \equiv 1,3 \bmod 8$$

$$p \mid x^2 + 3y^2 \text{ where } \gcd(x,y) = 1 \iff \left(\frac{-3}{p}\right) = 1 \text{ or } p = 3 \iff p \equiv 0,1 \bmod 3$$

*Proof.* Lemma 1.1.2 immediately yields us the equivalences on the left hand side. By using Theorem 1.1.4, we find that we have $\left(\frac{-1}{p}\right) = 1$ if and only if $\frac{p-1}{2} \equiv 0 \bmod 2$, which is the case if and only if $p \equiv 1 \bmod 4$.

Using the multiplicity of the Legendre symbol, we find that $\left(\frac{-2}{p}\right) = 1$ if and only if $\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$. By Theorem 1.1.4, we see that this happens exactly when $(-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = 1$, or equivalently $p \equiv 1,3 \bmod 8$. In the same way we find that $\left(\frac{-3}{p}\right) = 1$ if and only if $(-1)^{(p-1)/2}\left(\frac{3}{p}\right) = 1$, which by Theorem 1.1.4 is equivalent to saying $\left(\frac{p}{3}\right) = 1$. So we find that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 3$. □

The second step of the proof is the Descent step. We prove that an odd prime number dividing a number $N = a^2 + nb^2$, where $a$ and $b$ are coprime, is of the form $x^2 + ny^2$. We again first need a lemma before we can prove the final result. Let us first note the following fact.

**Remark 1.1.6.** *Let $n, x, y, z, w$ be integers, then*

$$(x^2 + ny^2)(w^2 + nz^2) = (xw \pm nyz)^2 + n(xz \mp yw)^2.$$

The identity in Remark 1.1.6 shows that if we multiply two numbers of the form $x^2 + ny^2$, their product is of this form as well. We will use this fact to divide out primes of this form.

**Lemma 1.1.7.** *Let $n \leq 3$ be a positive integer. Suppose we have $N = a^2 + nb^2$ for some coprime integers $a, b$ and let $q = x^2 + ny^2$ be a prime number dividing $N$. Then we have $\frac{N}{q} = c^2 + nd^2$ for some coprime integers $c, d$.*

*Proof.* We have $x^2N - a^2q = n(bx - ay)(bx + ay)$. In case we have $q \mid n$, it follows that $q = n$ and thus we find

$$\frac{N}{q} = \frac{a^2}{n} + b^2 = b^2 + n\left(\frac{a}{n}\right)^2.$$

Otherwise we have $q \mid bx - ay$, where we can change the sign of $a$ if necessary, so $bx - ay = dq$ for some integer $d$. Now we have

$$(a + ndy)y = ay + ndy^2 = bx - d(q - ny^2) = bx - dx^2.$$

This implies $x \mid a + ndy$, so $a + ndy = cx$ for some integer $c$.

Consequently we now have $a = cx - ndy$ and $b = cy + dx$. By Remark 1.1.6 we find

$$N = a^2 + nb^2 = (cx - ndy)^2 + n(cy + dx)^2 = (c^2 + nd^2)(x^2 + ny^2) = q(c^2 + nd^2).$$ □

**Remark 1.1.8.** *A similar result holds if $N = a^2 + 3b^2$ for some coprime integers $a, b$ and we have $4 \mid N$. In this case, we find that we have $N \equiv a^2 + 3b^2 \equiv a^2 - b^2 \bmod 4$ and thus*

$$a^2 \equiv b^2 \bmod 4.$$

*Now, either $a$ and $b$ are both even, in which case we have $\frac{N}{4} = (\frac{a}{2})^2 + 3(\frac{b}{2})^2$, or both are odd. In this case, by changing the sign of $a$ if necessary, we find that we have $4 \mid b - a$ and so $b - a = 4d$ for some integer $d$. By defining $c = a + 3d$, we then find $b = c + d$ and $a = c - 3d$. Using the identity in Remark 1.1.6, we find*

$$N = a^2 + 3b^2 = (c - 3d)^2 + 3(c + d)^2 = 4(c^2 + 3d^2).$$

Using Lemma 1.1.7 we can now prove the Descent step for the cases where $n \leq 3$.

**Proposition 1.1.9.** *(Descent step) Let $n \leq 3$ and let $p$ be an odd prime number. If we have $p \mid N$ where $N = X^2 + nY^2$ for some integers $X, Y$ with $gcd(X, Y) = 1$, then $p$ can be writen as $p = x^2 + ny^2$.*

*Proof.* We may assume we have $|X|, |Y| < \frac{p}{2}$ and thus $N < \frac{n+1}{4}p^2$, since we can first take numbers congruent to $X$ and $Y$ modulo $p$ which satisfy this condition, and then divide them by their greatest common divisor $d$, which is necessarily smaller than $p$. So we find that, for any odd prime $q \neq p$ with $q \mid N$, we have $q < p$.

We first consider the case where $q = 2$. We see that for $n = 1, 2$ we have that $q$ is of the form $x^2 + ny^2$ and thus by Lemma 1.1.7 it follows that $\frac{N}{2}$ is also of the form $X^2 + nY^2$. In the case where $n = 3$, we find that we have $N \equiv X^2 - Y^2 \bmod 4$ and thus $N \not\equiv 2 \bmod 4$. This means that $2 \mid N$ implies we have $4 \mid N$, and by Remark 1.1.8 we find that $\frac{N}{4}$ is also of the form $X^2 + nY^2$.

Now if $p$ is not of the form $x^2 + ny^2$, then by Lemma 1.1.7 and above argument, we find that there is an odd prime number $q < p$ such that $q$ is not of the form $x^2 + ny^2$. This means we get an infinite descending sequence of odd primes. This is not possible, so we find that $p$ is of the form $x^2 + ny^2$. □

We can now combine the Reciprocity step and the Descent step to give a result in which cases we can write a prime as $x^2 + ny^2$ for $n = 1, 2, 3$.

**Theorem 1.1.10.** *Let $p$ be an odd prime number. Then*

$$p = x^2 + y^2 \quad \iff \quad p \equiv 1 \bmod 4$$

$$p = x^2 + 2y^2 \quad \iff \quad p \equiv 1, 3 \bmod 8$$

$$p = x^2 + 3y^2 \quad \iff \quad p \equiv 0, 1 \bmod 3$$

*Proof.* Follows immediately from combining Proposition 1.1.5 and Proposition 1.1.9. □

**Remark 1.1.11.** *If we consider odd primes of the form $x^2 + 4y^2$, we see that these primes can be written as $x^2 + (2y)^2$. Since for any odd prime of the form $x^2 + y^2$ we have that either $x$ or $y$ is odd, we find that an odd prime is of the form $x^2 + 4y^2$ if and only if it is of the form $x^2 + y^2$.*

## 1.2 Cubic and biquadratic reciprocity

If one studies quadratic reciprocity more closely, it is not very hard to see that for any odd prime $p$ the Legendre symbol $\left(\frac{a}{p}\right)$ denotes the unique root of the polynomial $x^2 - 1$ congruent to $a^{(p-1)/2}$, whenever $a$ and $p$ are coprime. In this section, we will show that this can be generalized for primes in larger integer rings, where integers $a$ are related to third and fourth roots of unity. We will then show how this theory relates to our Main Theorem.

First let us introduce the rings we will study. Let $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$ denote a third root of unity and let $i$ denote a fourth root of unity in the field of complex numbers. Now we will study $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$, which are subrings of the complex numbers. We will later show that these rings are related to field extensions of $\mathbb{Q}$, by noting that these rings are the rings of algebraic integers of the quadratic fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(i)$ respectively (see Example 3.1.3).

Let us list the most important properties of these rings, which we will use to find more results on primes of the form $x^2 + ny^2$. For this, we first need to introduce the norm of an element $\alpha$ in one of these rings. We define the norm $N(\alpha)$ to be $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate.

**Proposition 1.2.1.** *Let $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ be rings contained in $\mathbb{C}$, where $\omega$ and $i$ are primitive third and fourth roots of unity, respectively. Then the following statements hold.*

1. *The rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are both principal ideal domains and unique factorization domains.*
2. *Let $\pi \in \mathbb{Z}[\omega]$ be a prime not dividing 3. Then $N(\pi) \equiv 1 \bmod 3$.*
3. *Let $\pi \in \mathbb{Z}[i]$ be a prime not dividing 2. Then $N(\pi) \equiv 1 \bmod 4$.*

*Proof.* For statement 1., see [Cox13, Cor. 4.4, p. 68] and [Ste10, Thm. 12.19, p. 29], for statement 2. see [Cox13, Prop. 4.7, p. 69] and for statement 3. see [Cox13, Prop. 4.18, p. 73]. □

For any prime $\pi \in \mathbb{Z}[\omega]$ not dividing 3, it is easy to see that $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field with $N(\pi)$ elements. This implies that $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$ for any $\alpha$ coprime to $\pi$. Since $N(\pi) \equiv 1 \bmod 3$ by statement 2. of Proposition 1.2.1, this implies that $\alpha^{(N(\pi)-1)/3}$ is a third root of unity modulo $\pi$.

If $\pi$ does not divide 3, it follows that $x^3 - 1$ is separable modulo 3, which implies that each $\alpha \in \mathbb{Z}[\omega]$ prime to $\pi$ is congruent to a unique third root of unity modulo $\pi$. In a similar way, we see that, for any $\beta \in \mathbb{Z}[i]$ coprime to a prime $\pi' \in \mathbb{Z}[i]$ not dividing 2, $\beta$ is congruent to a unique fourth root of unity modulo $\pi'$.

**Definition 1.2.2.** *(Legendre symbol)*

1. *Let $\pi \in \mathbb{Z}[\omega]$ be a prime not dividing 3 and let $\alpha \in \mathbb{Z}[\omega]$ be a number not divisible by $\pi$. Then the (cubic)* Legendre symbol $\left(\frac{\alpha}{\pi}\right)_3$ *is defined as the unique third root of unity such that*

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi.$$

2. *Let $\pi \in \mathbb{Z}[i]$ be a prime not dividing 2 and let $\alpha \in \mathbb{Z}[i]$ be a number not divisible by $\pi$. Then the (biquadratic)* Legendre symbol $\left(\frac{\alpha}{\pi}\right)_4$ *is defined as the unique fourth root of unity such that*

$$\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \bmod \pi.$$

The quadratic reciprocity law has equivalent statements, which hold for cubic and biquadratic Legendre symbols. We will state them without a proof, which can be found in [IR82, Ch. 9, p. 108].

**Theorem 1.2.3.** *(Cubic and biquadratic reciprocity law)*

1. *Let $\pi, \rho \in \mathbb{Z}[\omega]$ be primes with distinct norm such that both primes are congruent to $\pm 1$ modulo 3, then*

$$\left(\frac{\pi}{\rho}\right)_3 = \left(\frac{\rho}{\pi}\right)_3.$$

2. *Let $\pi, \rho \in \mathbb{Z}[i]$ be distinct primes such that both primes are congruent to 1 modulo $(1+i)^3$, then*

$$\left(\frac{\rho}{\pi}\right)_4 = \left(\frac{\pi}{\rho}\right)_4 (-1)^{(N(\rho)-1)(N(\pi)-1)/16}.$$

One might wonder if there are similar theorems for rings containing a $n$-th root of unity for larger values of $n$. The main problem that arises, is that these rings are in general no longer unique factorization domains. However, it is still possible to prove a more general reciprocity theorem for arbitrary values of $n$, which will be given in section 3.4.2. These results will be stated in terms of ideals, rather than elements, as ideals still do have a unique factorization in these larger rings. These results can also be used to prove Theorem 1.2.3.

If we return to our question about primes of the form $x^2 + ny^2$, we see that, for a prime $\pi \in \mathbb{Z}[\omega]$, the Legendre symbol for an element $\alpha \in \mathbb{Z}[\omega]$ equals 1 if and only if $\alpha$ is a cubic residue modulo $\pi$. In $\mathbb{Z}[i]$, we have that $\alpha$ will be a biquadratic residue if its Legendre symbol is 1. This allows us to proof results about primes of the form $x^2 + 27y^2$ and $x^2 + 64y^2$, which are strongly connected to the rings by the factorization $x^2 + 27y^2 = (x + 3\sqrt{-3}y)(x - 3\sqrt{-3}y)$ and $x^2 + 64y^2 = (x + 8iy)(x - 8iy)$. For a proof one should consult Cox, see [Cox13, Thm. 4.15 and Thm. 4.23, p. 72 and p. 74].

**Theorem 1.2.4.** *Let $p$ be a prime. Then*

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

$$p = x^2 + 64y^2 \iff p \equiv 1 \bmod 4 \text{ and } 2 \text{ is a biquadratic residue modulo } p. \qquad \square$$

Again one might wonder if generalization for $n$-th roots of unity and corresponding reciprocity laws yields more results. The key ingredient of the proof however, is the factorization in the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ of these primes. For larger values of $n$, the fields containing such roots will be extensions of degree larger than 2. So we will need different methods for proving our Main Theorem for arbitrary values of $n$.

# Chapter 2

# Quadratic forms

Lagrange was the first to study quadratic forms, which are polynomials of degree 2 in two variables. Introducing some basic definitions and an equivalence relation, he managed to provide tools for answering more questions about primes represented by the form $x^2+ny^2$. It will provide a different proof of the results from Chapter 1, but also results of an equivalent form for different values of $n$. We will also study the work of Gauss, in which he managed to construct a group law on the set of proper equivalence classes of quadratic forms. Finally, we will discuss how these results can be used to determine in which cases a congruence condition of $p$ modulo $4n$ is sufficient to ensure a prime is of the form $x^2+ny^2$, which turns out to happen only in finitely many cases.

## 2.1 Quadratic forms

In order to study wether a prime can be expressed by the form $x^2+ny^2$ whenever $n \geq 5$, we will look more closely at the expression $x^2+ny^2$. As a polynomial in two variables $x$ and $y$, it is a quadratic form.

**Definition 2.1.1.** *(Quadratic form) Let $a, b, c \in \mathbb{Z}$ be integers. A* quadratic form *is a polynomial $f(x, y)$ in 2 variables $x, y$ such that*

$$f(x, y) = ax^2 + bxy + cy^2.$$

*A quadratic form is called* primitive *if we have* $\gcd(a, b, c) = 1$.

We will study the quadratic form $x^2+ny^2$, in order to look for prime numbers that can be represented by this form. For this we will first need to determine in which cases prime numbers are represented by a certain quadratic form. We will then introduce a method to relate different quadratic forms by an equivalence relation. This will tell us which primes are represented by the form $x^2+ny^2$ for some values of $n$.

**Definition 2.1.2.** *Let $m \in \mathbb{Z}$ be an integer and let $f(x, y)$ be a quadratic form. We say that $m$ is* represented by *$f(x, y)$ if there are integers $p, q \in \mathbb{Z}$ such that*

$$m = f(p, q).$$

*Furthermore, we will say that $m$ is* properly *represented if we also have that* $\gcd(p, q) = 1$.

**Definition 2.1.3.** *(Discriminant) Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form. The* discriminant *$D$ of $f(x, y)$ is defined as*

$$D = b^2 - 4ac.$$

Before studying which forms represent certain integers, and in particular prime numbers, we need to find a way to group together forms representing the same set of numbers, to give us a more conclusive result about whether or not a certain form represents an integer. For this purpose, we introduce the following equivalence of quadratic forms.

**Definition 2.1.4.** *(Equivalent forms) Let $f(x,y)$ and $g(x,y)$ be quadratic forms. We say that $f(x,y)$ and $g(x,y)$ are* equivalent *if there are $p,q,r,s \in \mathbb{Z}$ such that*

$$f(x,y) = g(px+qy, rx+sy) \text{ and } ps-qr = \pm 1.$$

*If $ps-qr=1$, we say that $f(x,y)$ and $g(x,y)$ are* properly equivalent*.*

**Remark 2.1.5.** *The relation defined in Definition 2.1.4 indeed defines an equivalence relation.*

One can easily check this, by noting that a quadratic form can be uniquely represented by a $2\times 2$ matrix $A$, and the integers $p,q,r,s$ correspond with invertible matrices with integer coeffecients, whose inverses also have integer coeffecients. This fact can also be used to show some properties that equivalent forms share. For any two equivalent forms, we will see that they represent the exact same set of numbers. Moreover, they also have the same discriminant.

**Proposition 2.1.6.** *Let $f(x,y)$ and $g(x,y)$ be two equivalent quadratic forms. Then an integer $m$ is represented by $f(x,y)$ if and only if it is represented by $g(x,y)$, both forms have the same discriminant and $f(x,y)$ is primitive if and only if $g(x,y)$ is primitive.*

*Proof.* Let $m$ be an integer represented by $f(x,y)$ and let $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0,y_0)=m$. Then there are integers $p,q,r,s$ such that $g(px_0+qy_0, rx_0+sy_0) = f(x_0,y_0) = m$, so $m$ is represented by $g(x,y)$.

Let $g(x,y) = ax^2+bxy+cy^2$ and let $p,q,r,s \in \mathbb{Z}$ such that $f(x,y) = g(px+qy, rx+sy)$. Consider the matrix $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. Then we see that $g(x,y) = \begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}$. The determinant of $A$ multiplied by $-4$ exactly yields the discriminant of $g(x,y)$. Since the matrix representing $f(x,y)$ is obtained by multiplying $A$ with invertible matrices, such that both the matrix and its inverse have integer coefficients, we find that $f(x,y)$ has the same discriminant.

Now suppose $f(x,y)$ is not primitive. Then there is some integer $d>1$ such that $d$ divides all coefficients of $f(x,y)$. This means that any number represented by $f(x,y)$ will be divisible by $d$ and so any number represented by $g(x,y)$ will be divisible by $d$ as well. For $g(x,y) = ax^2+bxy+cy^2$ this means that $a = g(1,0)$, $b = g(0,1)$ and $a+b+c = g(1,1)$ are all divisible by $d$, so we find that $g(x,y)$ is not primitive either. □

We can now turn into looking which primes can be expressed by the form $x^2+ny^2$. For this we will first need a lemma, after which we can prove a theorem about integers $m$ being represented by quadratic forms with discriminant $D$.

**Lemma 2.1.7.** *Let $f(x,y)$ be a quadratic form and let $m \in \mathbb{Z}$ be an integer. Then $m$ is properly represented by $f(x,y)$ if and only if $f(x,y)$ is properly equivalent to the form $mx^2+bxy+cy^2$ for some $b,c \in \mathbb{Z}$.*

*Proof.* First suppose that $f(x,y)$ properly represents $m$. Then there are some integers $p,r \in \mathbb{Z}$ with $\gcd(p,r)=1$ and $f(p,r)=m$. Since we have $\gcd(p,r)=1$, we can find integers $q,s \in \mathbb{Z}$ such that $ps-qr=1$. Now we have

$$\begin{aligned} f(px+qy,rx+sy) &= a(px+qy)^2+b(px+qy)(rx+sy)+c(rx+sy)^2 \\ &= (ap^2+bpr+cr^2)x^2+bxy+cy^2 = mx^2+bxy+cy^2 \end{aligned}$$

for some $b,c \in \mathbb{Z}$. So we find that $f(x,y)$ is properly equivalent to this form.

Suppose $f(x,y)$ is properly equivalent to $mx^2+bxy+cy^2$ for some $b,c \in \mathbb{Z}$. This form properly represents $m$ (by setting $(x,y)=(1,0)$), so $f(p,r)=m$ for some $p,r \in \mathbb{Z}$ with $\gcd(p,r)=1$. □

**Corollary 2.1.8.** *Let $n \in \mathbb{N}$ be a positive integer and let $p$ be an odd prime not dividing $n$. Then $p$ is properly represented by a primitive form with discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right)=1$.*

*Proof.* First let us note that $\left(\frac{-4n}{p}\right)=\left(\frac{-n}{p}\right)$. If $p$ is properly represented by $f(x,y)$ with discriminant $-4n$, then by Lemma 2.1.7 we find $f(x,y)$ is properly equivalent to a form $px^2+bxy+cy^2$, where $-4n=D=b^2-4pc$. This implies $\left(\frac{-4n}{p}\right)=1$.

In case we have $\left(\frac{-n}{p}\right)=1$, we find that $-n=b^2-cp$ for some $b,c \in \mathbb{Z}$ and thus $-4n=(2b)^2-4cp$. Now the form $f(x,y)=px^2+2bxy+cy^2$ has discriminant $-4n$ and is primitive, since $p$ odd and not dividing $n$ implies $p$ not dividing $-4n$, from which follows that $p$ does not divide $2b$. □

We can now conclude in which case a prime $p$ can be represented by a quadratic form of discriminant $-4n$. Since $x^2+ny^2$ has discriminant $-4n$, we see that for any prime number of this form we necessarily have $\left(\frac{-n}{p}\right)=1$. However, we can not yet say anything about whether or not a prime with this property is actually represented by the particular form $x^2+ny^2$, or by some other form of the same discriminant. In order to do this, we will study the reduced forms, which will tell us more about whether or not $p$ can be represented by $x^2+ny^2$.

## 2.2 Reduced forms

We will introduce the concept of reduced forms, in order to show that every quadratic form is properly equivalent to a unique reduced form. This enables us to only study the reduced forms and the numbers they represent. Then, we look at the special reduced form $x^2+ny^2$, which is our main topic of interest. This leads us to a new result for primes represented by this form in the case where $n=7$.

First, we study the forms representing only positive values. Using the identity

$$4af(x,y)=4a^2x^2+4abxy+4acy^2=(2ax+by)^2-Dy^2,$$

we find that a form has discriminant $D<0$ and coeffecient $a>0$ if and only if all values represented by $f(x,y)$ for $(x,y) \neq (0,0)$ are positive.

**Definition 2.2.1.** *(Positive definite) Let $f(x,y)$ be a quadratic form. We say that $f(x,y)$ is* positive definite *if $f(x,y)$ represents only positive numbers for $(x,y) \neq (0,0)$.*

Note that in the same way we can define negative definite and indefinite forms, which represent negative and both positive and negative numbers, respectively. We can now give a definition of a reduced form.

**Definition 2.2.2.** *(Reduced form) Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive positive definite form. We say that $f(x,y)$ is* reduced *if*

$$|b| \leq a \leq c \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c.$$

In order to show the uniqueness of the reduced forms, we will need to show that no two reduced forms are properly equivalent. To show this, we observe that for a reduced form $f(x,y) = ax^2 + bxy + cy^2$ for which we have $|b| < a < c$, we find that $a$ and $c$ are the smallest values represented by $f(x,y)$. In case one of the equalities $|b| = a$ or $a = c$ holds, we can find similar results by observing that $a$ still is the smallest number represented by $f(x,y)$ and using that $b \geq 0$ in this case. This leads to the following lemma.

**Lemma 2.2.3.** *Let $f(x,y)$ and $g(x,y)$ be reduced quadratic forms. If $f(x,y)$ and $g(x,y)$ are properly equivalent, then $f(x,y) = g(x,y)$.*

We can now state our main theorem on quadratic forms, which yields us a way to uniquely represent a proper equivalence class of primitive positive forms.

**Theorem 2.2.4.** *Every primitive positive definite quadratic form is properly equivalent to a unique reduced form.*

*Proof.* Let $f(x,y)$ be a quadratic form. Among all of the forms properly equivalent to $f(x,y)$, choose the form $g(x,y) = ax^2 + bxy + cy^2$ with the smallest value of $|b|$.

First suppose that we have $a < |b|$. The forms $g(x \pm y, y) = ax^2 + (b \pm 2a)xy + (a + c)y^2$ are properly equivalent to $f(x,y)$ and since we have that either $|b+2a| < |b|$ or $|b-2a| < |b|$ by the assumption $0 \leq a < |b|$, we get a contradiction. So we find that we have $a \geq |b|$ and by using that $g(x,y)$ and $g(-y,x)$ are properly equivalent we find $c \geq |b|$ using the same argument. We can also use this equivalence to obtain $c \geq a$, so $f(x,y)$ is properly equivalent to a reduced form or to a form $h(x,y) = a'x^2 + b'xy + c'y^2$, such that its coefficients satisfy $|b'| \leq a' \leq c'$, $b' < 0$, and $|b'| = a'$ or $a' = c'$. In case we have $|b'| = a'$, we find that the form $h(x + y, y)$ is properly equivalent to $f(x,y)$ and is reduced and in the case we have $h(x,y)$ with $a' = c'$, we find that the form $h(-y,x)$ is properly equivalent to $f(x,y)$ and is reduced. By Lemma 2.2.3, this reduced form is not properly equivalent to any other reduced form, and thus uniqueness follows. □

Since we have $D = b^2 - 4ac \geq -3a^2$ for any reduced form and thus $a^2 \leq -D/3$, we see that the number of reduced forms with discriminant $D$ is finite. This means Theorem 2.2.4 implies that the amount of proper equivalence classes of primitive positive definite forms with fixed discriminant $D$ is finite. We will denote the amount of reduced forms, which equals the amount of proper equivalence classes, with discriminant $D < 0$ by $h(D)$.

By combining Corollary 2.1.8 and Theorem 2.2.4, we now find that for any odd prime $p$ satisfying $\left(\frac{-n}{p}\right) = 1$, the prime $p$ is represented by a reduced form with discriminant $-4n$. This means we know when a prime will be represented by a reduced form with discriminant $-4n$, but we have no way yet to determine which quadratic form will represent $p$ in case $h(D) > 1$. Since $h(-4n) = 1$ if and only if $n \in \{1, 2, 3, 4, 7\}$, which can be shown by constructing two reduced forms of discriminant $-4n$ for all other values of $n$, we will need a way to distinguish reduced forms and their corresponding proper equivalence classes of forms for a stronger result.

## 2.3 Genus theory

Consider the quadratic form $x^2 + ny^2$ with discriminant $D = -4n$. This form is reduced for all positive integers $n$, which turns us into looking for a way to distinguish the reduced forms and by that distinguish all proper equivalence classes of forms. This will be the study of Genus Theory, a name which comes from Gauss ([Cox13, p. 59]).

**Example 2.3.1.** *Let $m$ be an integer represented by $x^2 + 5y^2$, and coprime to the discriminant $D = -20$ of the form. We find that $m \equiv x^2 \bmod 5$ and $m \equiv x^2 + y^2 \bmod 4$, which implies $m \equiv \pm 1 \bmod 5$ and $m \equiv 1 \bmod 4$. So we find that $m \equiv 1, 9 \bmod 20$. Similar congruence arguments show that integers represented by $2x^2 + 2xy + 3y^2$, another reduced form with discriminant $D = -20$, are congruent to 3 or 7 modulo 20.*

We attempt to group together forms with discriminant $D < 0$ by the values in $(\mathbb{Z}/D\mathbb{Z})^*$ they represent. To do so, we first need a formal way to talk about the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented in the form, which is actually a coset of some subgroup of $(\mathbb{Z}/D\mathbb{Z})^*$. To show this, we first define the principal form.

**Definition 2.3.2.** *(Principal form) Let $n$ be a positive integer and let $D = -4n$. The* principal form *of discriminant $D$ is defined to be $x^2 + ny^2$.*

**Lemma 2.3.3.** *Let $f(x, y)$ be a primitive positive definite quadratic form with discriminant $D = -4n$. Let $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ be the unique homomorphism as determined by Theorem 1.1.3. Then the set of values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant $D$ form a subgroup $H \subset \ker\chi \subset (\mathbb{Z}/D\mathbb{Z})^*$ and the set of values represented by $f(x, y)$ form a coset of $H$ in $\ker\chi$.*

*Proof.* Suppose we have $m$ coprime to $D$ such that $m$ is represented by $f(x, y)$. If $m$ is not properly represented, let $d$ be the gcd of the pair $(x, y)$ representing $m$, then we can write $m = d^2m'$, where $m'$ is properly represented by $f(x, y)$, and we have $\chi(\overline{m}) = \chi(\overline{d})^2\chi(\overline{m'}) = \chi(\overline{m'})$. So, we may assume that $m$ is properly represented by $f(x, y)$. Then from Lemma 2.1.7, we can derive that $D$ is a quadratic residue modulo $m$, so $D = b^2 + km$ for some $b, k \in \mathbb{Z}$. Now, for any prime $p$ dividing $m$, we have $D \equiv b^2 \bmod p$ and thus $\chi(\overline{p}) = 1$ for all primes $p$ dividing $m$, which implies $\chi(\overline{m}) = 1$.

If we look at Remark 1.1.6, we see that the product of any two values in $\ker\chi$ represented by the principal form is again represented by it. So, we find that the values represented by the principal form indeed form a subset $H \subset \ker\chi$. For $a = f(1, 0)$, $b = f(0, 1)$ and $a + b + c = f(1, 1)$, we have $\gcd(a, b, a + b + c) = \gcd(a, b, c) = 1$. This implies that at least one of the values $f(1, 0), f(0, 1)$ and $f(1, 1)$ is coprime to $D$ and properly represented by $f(x, y)$, so, by Lemma 2.1.7, we can write $g(x, y) = a'x^2 + b'xy + c'xy$ where $g(x, y)$ is properly equivalent to $f(x, y)$ and $a'$ is coprime to $D$. Since $D = -4n$ is even, we find that $b'$ is even so that $b' = 2b''$, and we have

$$a'g(x, y) = (a'x + b''y)^2 + ny^2.$$

But this immediately implies that any value coprime to $D$ represented by $g(x, y)$, and therefore any value coprime to $D$ represented by $f(x, y)$ in $(\mathbb{Z}/D\mathbb{Z})^*$, lies in the coset $\overline{a'}^{-1}H$. □

Consequently, we see that we can group primitive positive definite forms with the same discriminant by the values in $(\mathbb{Z}/D\mathbb{Z})^*$ they represent.

**Definition 2.3.4.** *(Genus) Let $f(x, y)$ be a primitive positive definite quadratic form. The set of (equivalence classes of) forms representing a coset of $H \subset (\mathbb{Z}/D\mathbb{Z})^*$ as in Lemma 2.3.3, is called the* genus *of $f(x, y)$. The genus containing (the equivalence class of) the form $x^2 + ny^2$ is called the* principal genus.

For the cases where the principal genus consists of only one class, this gives us a result on when a prime $p$ can be written as $x^2 + ny^2$. However, two problems arise here. First, we have no way to compute for which values of $n$ this will happen. Moreover, one can show that only in a finite amount of cases the principal genus will consist of only one form. Therefore, we will need a more general approach to solve the problem.

## 2.4 Composition of forms

It is possible to compose the proper equivalence classes of forms, such that this composition defines a group law on this set. The corresponding group will later turn out to have very tight connections to the general solution of the question whether an odd prime $p$ can be expressed in the form $x^2 + ny^2$. Now, for two primitive positive definite quadratic forms $f(x, y)$ and $g(x, y)$ with the same discriminant $D = -4n$, we will define a composition of forms. We will first need a condition on the coefficients to get a direct expression for the composite form. For this, we will use the following lemma, which can be proven by rewriting the congruences to a general form and showing this general form has a unique solution.

**Lemma 2.4.1.** *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be two quadratic forms with discriminant $D$. Suppose we have $\gcd(a, a', (b + b')/2) = 1$. Then there is a unique integer $B$ modulo $2aa'$ such that we have*

$$B \equiv b \bmod 2a, B \equiv b' \bmod 2a' \text{ and } B^2 \equiv D \bmod 4aa'.$$

**Definition 2.4.2.** *(Dirichlet composition) Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be two primitive positive definite quadratic forms with discriminant $D < 0$ such that $\gcd(a, a', (b + b')/2) = 1$. We define the* Dirichlet composition *of the two forms to be the form*

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2$$

*where $B$ is the integer as found in Lemma 2.4.1, so that $F(x, y)$ is well-defined.*

One can immediately see that $F(x, y)$ is again a primitive positive definite form of discriminant $D$. We also see that, for any primitive positive definite form $f(x, y) = ax^2 + bxy + y^2$ with discriminant $D = -4n$, we have that $f(x, y)$ composed with the principal form $x^2 + ny^2$ gives $a' = 1$, and we see $B = b$ satisfies all congruences in Lemma 2.4.1 (where $b$ is even since $D = -4n$), so their Dirichlet composition will be $f(x, y)$. If we consider the opposite form $\tilde{f}(x, y) = ax^2 - bxy + cy^2$, we see that $\tilde{f}(-y, x) = cx^2 + bxy + ay^2$ is properly equivalent to it, and $B = b$ again satisfies all congruences in Lemma 2.4.1, which shows that their Dirichlet composition is $F(x, y) = acx^2 + bxy + y^2$. Since $F(-y, x + by/2) = x^2 + ny^2$, composing a form with its opposite yields the principal form.

These properties seem to suggest that Dirichlet composition defines a group law on the set of proper equivalence classes of primitive positive definite quadratic forms with discriminant $D = -4n$. For now, we will assume that Dirichlet composition indeed induces a well-defined group law on this set, which can be proven directly. A more convenient approach to proving this is by showing that there is a natural bijection between the form class group of discriminant $D$ and the ideal class group of an order with discriminant $D$ in an imaginary quadratic field. One can then show that ideal multiplication corresponds with Dirichlet composition on the related forms. This will be shown in section 3.4.1.

**Theorem 2.4.3.** *Let $D = -4n$ and denote by $C(D)$ the set of equivalence classes of primitive positive definite quadratic forms with discriminant $D$. Then Dirichlet composition defines a group law on $C(D)$ with the class of $x^2 + ny^2$ being the identity element. Furthermore, for any form $f(x, y)$, its opposite form $f'(x, y)$ is its inverse under this operation.*

We see that the form class group $C(D)$ with Dirichlet composition is now a finite abelian group. Since for an element in a group we have that its order is at most 2 if and only if the element is its own inverse, we see that for any class it is of order 2 in $C(D)$ if and only if the reduced form $f(x, y)$ representing the class is properly equivalent to its opposite. By looking at the proof of Theorem 2.2.4, we see that the opposite form is properly equivalent to $f(x, y)$ if and only if $b = 0$, $a = b$ or $a = c$.

Notice that we can compare the group structure of the form class group to that of the group of values represented by the corresponding forms. The principal genus then consists of the forms representing values in the subgroup $H \subset \ker \chi$ as found in Lemma 2.3.3. This means we obtain a homomorphism

$$\Phi : C(D) \to \ker \chi / H,$$

that sends any class of forms to the coset of values it represents. This is clearly a homomorphism, as any number represented by the Dirichlet composition $F(x, y)$ of two forms $f(x, y)$ and $g(x, y)$ can be written as a product of numbers represented by $f(x, y)$ and $g(x, y)$, and thus the coset of values represented by $F(x, y)$ is exactly the product of the cosets of values represented by $f(x, y)$ and $g(x, y)$, respectively. Another fact we can observe from this homomorphism, is that every genus consists of the same number of equivalence classes.

For any square integer we have that the principal form $f(x, y) = x^2 + ny^2$ represents it, as we have $f(x, 0) = x^2$. But this means that all squares in $(\mathbb{Z}/D\mathbb{Z})^*$ are contained in $H$ and thus every element in $\ker \chi / H$ has order at most 2. Thus, we find that the square of any form lies in the principal genus. We can show that the opposite also holds, so that any form in the principal genus can be written as a square. So this means we have a condition to ensure when we have only one form in the principal genus, since this is the case if and only if the subgroup of squares consists of one element. This happens if and only if all elements have order at most 2, which by above observations results into the following corollary.

**Corollary 2.4.4.** *Let $D = -4n$, then the following are equivalent:*

1. *The principal genus of reduced forms with discriminant $D$ consists of exactly one form.*
2. *Every reduced form of discriminant $D$ is properly equivalent to its opposite.*
3. *For every reduced form $ax^2 + bxy + cy^2$ with discriminant $D$, we have either $b = 0$, $a = b$ or $a = c$.*

*Proof.* The principal genus consists of exactly one form if and only if every element has order at most 2, which is the case if and only if every reduced form is properly equivalent to its opposite. Now a reduced form is properly equivalent to its opposite if and only if $b = 0$, $a = b$ or $a = c$, so the equivalences follow. □

This yields a more explicit way to compute the values of $n$ for which the principal genus of discriminant $-4n$ consists of just the principal form, as we can conclude whether or not this is the case by observing all reduced forms of discriminant $-4n$. However, computing the reduced forms still requires a lot of work, and it can be shown that only in a finite amount of cases we have that the principal genus consists of one form. This means that only in a finite number of cases we can determine whether a prime is of the form $x^2 + ny^2$ by considering just the residue class of the prime modulo $4n$. So, for other values of $n$, we will need to look for an additional condition on prime numbers to ensure a prime is of this particular form.

# Chapter 3

# Class field theory

This chapter covers some important theorems in two main subjects, algebraic number theory and class field theory. The first part will be focused on the behavior of prime ideals of the ring of algebraic integers in finite extensions of $\mathbb{Q}$. Then, we define the Artin symbol of a prime ideal, which will relate prime ideals to the Galois group of the extension. We introduce the concept of an order, so that we can study prime ideals in the ring $\mathbb{Z}[\sqrt{-n}]$, a ring that is tightly connected to our Main Theorem. Finally, we show the ideal class group of an order is isomorphic to the form class group of the same discriminant.

In the last section, we look into the theorems of class field theory. We define the Artin map and see how it relates the Galois group of an extension of number fields to the generalized ideal class group of the number field. This map allows us to construct abelian extensions of number fields, in which prime ideals ramify only if they divide a fixed ideal. These constructions will be crucial in proving the Main Theorem.

## 3.1 Algebraic number theory

Algebraic number theory is focused on the study of algebraic integers in number fields, which can be viewed as a generalization of the ring of integers $\mathbb{Z}$. We study the behavior of prime ideals in this ring, and their connection to algebraic numbers. Finally, we apply the results to quadratic fields, which are important for proving the Main Theorem.

### 3.1.1 Algebraic integers

To introduce the notion of an algebraic integer, we will first consider the fields we are interested in, which are finite extensions of $\mathbb{Q}$ which are embedded in $\mathbb{C}$.

**Definition 3.1.1.** *(Number Field) Let $K \subset \mathbb{C}$ be a subfield of the complex numbers such that $K$ is a finite extension of $\mathbb{Q}$. Then we say $K$ is a* number field.

**Definition 3.1.2.** *(Algebraic Integers) Let $K$ be a number field and let $\alpha \in K$. We say that $\alpha$ is an* algebraic integer *if there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $\alpha$ is a root of $f(x)$. The set of all* algebraic integers of $K$ *will be denoted by $\mathcal{O}_K$.*

**Example 3.1.3.** *Let $N \neq 0, 1$ be a squarefree integer and consider the field $K = \mathbb{Q}(\sqrt{N})$. Let $\alpha \in \mathcal{O}_K$, and denote by $f(x)$ the minimal polynomial of $\alpha$, then we have that $f(x) \in \mathbb{Z}[x]$. If we write $\alpha = a + b\sqrt{N}$, then we find that, by considering the non-trivial automorphism on $K$, the minimal polynomial $f(x)$ of $\alpha$ is given by*

$$(x - (a + b\sqrt{N}))(x - (a - b\sqrt{N})) = x^2 - 2ax + (a^2 - b^2N).$$

*Since the coefficients of this polynomial are integers, we find that $a \in \frac{1}{2}\mathbb{Z}$. If we write $a = \frac{m}{2}$ for some integer $m \in \mathbb{Z}$, we find $b^2N = \frac{4k+m^2}{4}$ for some integer $k \in \mathbb{Z}$. If $m$ is even, we find that both $a$ and $b$ are integers. For $m$ odd, it only has a solution if $N \equiv 1 \bmod 4$, in which case we find $b = \frac{n}{2}$ for some odd integer $n \in \mathbb{Z}$. So we conclude that*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \bmod 4. \end{cases}$$

**Definition 3.1.4.** *(Quadratic field) Let $K$ be a field of the form described in Example 3.1.3. Then $K$ is called a* quadratic field*. Furthermore we define the* discriminant *$d_K$ of $K$ to be*

$$d_K := \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{else.} \end{cases}$$

An important property of $\mathcal{O}_K$ is that it is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$ (see [Mar77, Cor. to Thm. 9, p. 29]). From this, we can derive a series of useful properties, which tell us that $\mathcal{O}_K$ is actually a Dedekind domain, and thus any ideal has a unique decomposition into prime ideals.

**Proposition 3.1.5.** *Let $K$ be a number field and let $\mathcal{O}_K$ be the set of algebraic integers of $K$. Then the following statements hold.*

1. *The set $\mathcal{O}_K$ is a subring of $\mathbb{C}$ and $K$ is its field of fractions.*
2. *For any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. The* norm *$N(\mathfrak{a})$ of $\mathfrak{a}$ is then defined as $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.*
3. *The ring $\mathcal{O}_K$ is a Dedekind domain.*

*Proof.* Let $K$ be a number field and let $\mathcal{O}_K$ be the algebraic integers of $K$.

1. Let $\alpha, \beta \in \mathcal{O}_K$. Since we have that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, it follows that $\mathbb{Z}[\alpha+\beta] \subset \mathcal{O}_K$, $\mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha, \beta] \subset \mathcal{O}_K$ and $\mathbb{Z}[-\alpha] \subset \mathcal{O}_K$. This immediately implies $\alpha+\beta, \alpha\beta, -\alpha \in \mathcal{O}_K$, and therefore we have that $\mathcal{O}_K$ is a ring contained in $\mathbb{C}$.

2. Let $\alpha \in \mathfrak{a}$ such that $\alpha \neq 0$ and let $f(X) \in \mathbb{Z}[X]$ be a polynomial such that $f(\alpha) = 0$. Now if $m$ is the constant coefficient of $f(X)$ we have $m \in \mathfrak{a}$, since $\alpha \in \mathfrak{a}$ and $f(\alpha) = 0$. But this implies we have $m\mathcal{O}_K \subset \mathfrak{a}$, and thus there is a surjection $\mathcal{O}_K/m\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$. Using that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, we find that $\mathcal{O}_K/m\mathcal{O}_K$ is finite from which immediately follows that $\mathcal{O}_K/\mathfrak{a}$ is finite.

3. We will show that $\mathcal{O}_K$ is a Dedekind domain by showing it is integrally closed in $K$, Noetherian and every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

   Suppose we have $f(X) \in \mathcal{O}_K[X]$ and $\alpha \in K$ such that $f(\alpha) = 0$. The ring $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathcal{O}_K$-module, and since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, we see that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. But this yields a monic polynomial $g(X) \in \mathbb{Z}[X]$ such that $g(\alpha) = 0$, which implies $\alpha \in \mathcal{O}_K$. Thus $\mathcal{O}_K$ is integrally closed in $K$.

   Suppose we have an infinite chain of ideal inclusions $0 = \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$. By property 2. we see that $\mathcal{O}_K/\mathfrak{a}_i$ is finite for all $i \geq 1$, which implies that there is $I \in \mathbb{N}$ such that $\mathfrak{a}_i = \mathfrak{a}_j$ for all $i, j > I$. So we find that $\mathcal{O}_K$ is Noetherian.

   Let $\mathfrak{p}$ be a prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a domain. Since it is finite by property 2., we find that $\mathcal{O}_K/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is a maximal ideal. □

### 3.1.2 Prime ideals

In Proposition 3.1.5, we saw that, for a number field $K$, the ring of integers $\mathcal{O}_K$ is a Dedekind domain. An important consequence of this fact is the unique factorization of ideals into prime ideals, which is a general result that holds in any Dedekind domain (see [Mar77, Thm. 16, p. 59]).

**Corollary 3.1.6.** *Let $K$ be a number field and let $\mathcal{O}_K$ be its ring of integers. Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then $\mathfrak{a}$ can be uniquely written as*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m$$

*were all of the $\mathfrak{p}_i$'s are nonzero prime ideals of $\mathcal{O}_K$.*

**Remark 3.1.7.** *For convenience, we will often refer to nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ as "primes of $K$".*

Suppose we have a finite extension $K \subset L$ of number fields. If $\mathfrak{p}$ is a prime of $K$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$, and, by Corollary 3.1.6, can therefore be uniquely factored into prime ideals of $\mathcal{O}_L$. Now write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, where the $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_L$. We say that the primes $\mathfrak{P}_i$ are the primes *lying over* $\mathfrak{p}$. The numbers $e_i$, also denoted by $e_{\mathfrak{P}_i|\mathfrak{p}}$, are called the *ramification indices* of $\mathfrak{p}$ in $\mathfrak{P}_i$. For any of the primes $\mathfrak{P}_i$, we define the *inertial degree* $f_{\mathfrak{P}_i|\mathfrak{p}}$ to be the degree of the extension $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$ of finite fields. We will see that these numbers are strongly related to the degree of the extension $K \subset L$.

**Theorem 3.1.8.** *Let $K \subset L$ be an extension of number fields, let $\mathfrak{p}$ be a prime of $K$ and denote by $e_i$ and $f_i$ the ramification indices and inertial degrees of the primes $\mathfrak{P}_i$ lying over $\mathfrak{p}$, respectively.*

1. *The following equality holds*
$$\sum_{i=1}^{g} e_i f_i = [L : K].$$
2. *If $K \subset L$ is Galois, then all primes $\mathfrak{P}$ lying over $\mathfrak{p}$ have the same ramification index $e$ and inertial degree $f$, and we have*
$$efg = [L : K].$$
*In this case, we define $e$ to be the* ramification index *and $f$ to be the* inertial degree of $\mathfrak{p}$ in $L$.

*Proof.* We will assume the norm function on ideals is multiplicative and the Galois group acts transitively on the primes in $L$ lying over the prime $\mathfrak{p}$ of $K$. For a proof of these facts, see [Mar77, Thm. 22 and Thm. 23, p. 66 and p. 70].

1. By computing the norms of the ideal $\mathfrak{p}\mathcal{O}_L$ and the prime ideals $\mathfrak{P}_i$, we find $N(\mathfrak{p}\mathcal{O}_L) = |\mathcal{O}_K/\mathfrak{p}|^n$ and $N(\mathfrak{P}_i^{e_i}) = |\mathcal{O}_K/\mathfrak{p}|^{e_i f_i}$. Hence, we find
$$\sum_{i=1}^{g} e_i f_i = [L : K].$$
2. Since $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$ for all $\sigma \in \mathrm{Gal}(L/K)$, we find that $e_{\mathfrak{P}_i|\mathfrak{p}} = e_{\sigma(\mathfrak{P}_i)|\mathfrak{p}} = e$ for all $1 \le i \le g$ and some integer $e$. In the same way, one finds that any $\sigma \in \mathrm{Gal}(L/K)$ induces an isomorphism between $\mathcal{O}_L/\mathfrak{P}_i$ and $\mathcal{O}_L/\sigma(\mathfrak{P}_i)$, and therefore $f_{\mathfrak{P}_i|\mathfrak{p}} = f_{\sigma(\mathfrak{P}_i)|\mathfrak{p}} = f$ for all $1 \le i \le g$ and some integer $f$. Consequently, by using the result from 1., we find that
$$efg = [L : K].$$
□

We see that the behavior of primes of $K$ in the extension $L$ is uniquely determined by the numbers $e$ and $f$. We will be mostly interested in the case where we have $e = 1$ and $f = 1$, which leads to the following definition.

**Definition 3.1.9.** *Let $K \subset L$ be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime in $K$ and let $e$ and $f$ be the ramification index and inertial degree of $\mathfrak{p}$ in $L$ respectively. If $e > 1$, we say* $\mathfrak{p}$ ramifies *in $L$; else we have $e = 1$, and we say that the prime $\mathfrak{p}$ is* unramified *in $L$. If $\mathfrak{p}$ is unramified in $L$ and we also have that $f = 1$, we say that* $\mathfrak{p}$ splits completely *in $L$.*

To prove our Main Theorem on primes of the form $x^2 + ny^2$, we first prove a theorem saying that an odd prime will be of this form if and only if the prime $p$ splits completely in a certain extension $L$ of the field $K = \mathbb{Q}(\sqrt{-n})$, called the ring class field. So, we will look for a condition on a prime $\mathfrak{p}$ of $K$ that ensures the prime will split completely in an extension $L$ of $K$. This results into the following proposition.

**Proposition 3.1.10.** *Let $K \subset L$ be a Galois extension of number fields, where we have $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$. Let $f(x)$ be the minimal polynomial of $\alpha$ over $K$. If $\mathfrak{p}$ is a prime of $K$ and $f(x)$ is separable modulo $\mathfrak{p}$, then the following statements hold.*

1. *If we let $f(x) \equiv f_1(x) \cdots f_g(x) \bmod p$, where the $f_i(x)$ are distinct monic irreducible polynomials modulo $\mathfrak{p}$, then for every $i$ we have that $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, all the $\mathfrak{P}_i$'s are distinct and we have*
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g.$$
*Furthermore, all the $f_i(x)$'s have the same degree which equals the inertial degree $f$ of $\mathfrak{p}$ in $L$.*

2. *The prime $\mathfrak{p}$ is unramified in $L$ and splits completely if and only if $f(x) \equiv 0 \bmod \mathfrak{p}$ has a solution in $\mathcal{O}_K$.*

*Proof.* We use the fact that for each prime $\mathfrak{P}$ lying over $\mathfrak{p}$, there are exactly $ef$ elements $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}$, which form a subgroup. This subgroup is called the decomposition group of $\mathfrak{P}$ and is denoted by $D_{\mathfrak{P}}$. For a proof, see [Mar77, Thm. 28, p. 100].

1. Since $f(\alpha) = 0 \mod \mathfrak{p}$, we find that for each prime $\mathfrak{P}$ lying over $\mathfrak{p}$ there is some $f_i(x)$ such that $f_i(\alpha) \in \mathfrak{P}$. Without loss of generality, we assume $f_1(\alpha) \in \mathfrak{P}$. Since $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$ by definition of $f$, and $f_1(x)$ is the minimal polynomial of the element $\alpha$ in this extension, we have $\deg(f_1(x)) \leq f$.

   Now, we have $f_1(\sigma(\alpha)) \equiv \sigma(f_1(\alpha)) \equiv 0 \bmod \mathfrak{P}$ for every $\sigma \in D_{\mathfrak{P}}$, and since $f(x)$ and thus $f_1(x)$ is separable, this means that $f_1(x)$ has $ef$ distinct zeroes in $\mathcal{O}_L/\mathfrak{P}$. So we find that $\deg(f_1(x)) \geq ef$. Both statements combined imply $e = 1$ and $\deg(f_1(x)) = f$, so we find that the number of distinct factors $f_i(x)$ equals the number $g$ of distinct primes $\mathfrak{P}_i$ lying over $\mathfrak{p}$.

   So we find that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, where $f_i(\alpha) \in \mathfrak{P}_i$ for all $1 \leq i \leq g$. If we let $I_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)$ for $1 \leq i \leq g$, we see that $I_i \subset \mathfrak{P}_i$ for all $i$, but at the same time we have $\mathfrak{P}_1 \cdots \mathfrak{P}_g = \mathfrak{p}\mathcal{O}_L \subset I_i$ for all $i$. From this we immediately find $I_i = \mathfrak{P}_i$ for all $i$, as $f_i(\alpha) \notin \mathfrak{P}_j$ for $i \neq j$, so that indeed we have $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)$ for all $i$.

2. Part 1. implies that $\mathfrak{p}\mathcal{O}_L$ is a product of distinct primes and thus $e = 1$, so $\mathfrak{p}$ is unramified.

   Suppose that $\mathfrak{p}$ splits completely, then we have $f = 1$ and by statement 1., we see that all the $f_i(x)$'s have degree 1 and thus have a zero in $\mathcal{O}_K$. Hence the equation $f(x) \equiv 0 \bmod \mathfrak{p}$ has a solution. Conversely, if $f(x) \equiv 0 \bmod \mathfrak{p}$ has a solution, we find some irreducible polynomial $f_i(x)$ modulo $\mathfrak{p}$ of degree 1 that divides $f(x)$, which when combined with statement 1. implies that $f = \deg f_i(x) = 1$. Therefore, $\mathfrak{p}$ splits completely. □

**Proposition 3.1.11.** *Let $K$ be a quadratic field and let $d_K$ be its discriminant. Let $p$ be an odd prime number.*

1. *If $\left(\frac{d_K}{p}\right) = 0$, we have $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.*
2. *If $\left(\frac{d_K}{p}\right) = -1$, we have that $p\mathcal{O}_K$ is prime in $\mathcal{O}_K$.*
3. *If $\left(\frac{d_K}{p}\right) = 1$, we have $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for some distinct prime ideals $\mathfrak{p}, \mathfrak{p}'$ in $\mathcal{O}_K$.*

*Proof.* First suppose we have $\left(\frac{d_K}{p}\right) = 0$, which is equivalent to $p \mid d_K$.

1. Let $\mathfrak{p} = p\mathcal{O}_K + \sqrt{d_K}\mathcal{O}_K$, then we have $\mathfrak{p}^2 = p\mathcal{O}_K$. Now by Theorem 3.1.8 we see that $\mathfrak{p}$ is necessarily prime.

Otherwise we have $\left(\frac{d_K}{p}\right) \neq 0$ and $K = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{d_K})$. By applying Proposition 3.1.10 to $\sqrt{d_K}$ and its minimal polynomial $X^2 - d_K$ which is separable modulo $p$ we find:

2. The condition $\left(\frac{d_K}{p}\right) = -1$ implies that $X^2 - d_K$ is irreducible modulo $p$, and thus $\mathfrak{p}\mathcal{O}_K$ is prime in $\mathcal{O}_K$.
3. Since $\left(\frac{d_K}{p}\right) = 1$, we have that $X^2 - d_K \equiv 0 \bmod p$ has a solution, and thus $\mathfrak{p}\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for some distinct prime ideals $\mathfrak{p}, \mathfrak{p}'$ in $\mathcal{O}_K$. □

The case where $p = 2$ is slightly different. If we have $2 \mid d_K$, one can show that $2\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Else, we have $d_K = N \equiv 1 \bmod 4$, and we have $K = \mathbb{Q}\left(\frac{1+\sqrt{d_K}}{2}\right)$. Then we can apply Proposition 3.1.10 to $\frac{1+\sqrt{d_K}}{2}$ and its minimal polynomial $X^2 + X + \frac{1-d_K}{4}$, which is separable modulo 2. This polynomial is irreducible modulo 2 if and only if $\frac{1-d_K}{4}$ is odd, so we find that 2 splits completely in $K$ if and only if $N = d_K \equiv 1 \bmod 8$; and $2\mathcal{O}_K$ is prime if and only if $d_K \equiv 5 \bmod 8$.

## 3.2 Hilbert class field

We now study more closely a condition that ensures when a prime $p$ can be written as $x^2 + ny^2$. There is a number field in which this condition is equivalent to the prime splitting completely. Since this means the prime is necessarily unramified, we will determine in which extensions of a field $K$ a prime is unramified. For this we first define infinite primes.

**Definition 3.2.1.** *(Infinite prime) An embedding $\sigma$ of $K$ into $\mathbb{R}$ is called a* real infinite prime. *A pair of conjugate embeddings $\sigma, \overline{\sigma}$ with $\sigma \neq \overline{\sigma}$ of $K$ into $\mathbb{C}$ is called a* complex infinite prime. *We say a real infinite prime of $K$* ramifies *in $L$ if there is an extension of $\sigma$ on $L$ that is complex. If such an extension does not exist, we say the real prime is* unramified *in $L$.*

**Definition 3.2.2.** *(Unramified extension) Let $K \subset L$ be an extension of number fields. We say the extension is* unramified *if every prime ideal of $\mathcal{O}_K$ and every infinite prime of $K$ is unramified in $L$.*

Unramified extensions are interesting, because of the behavior of prime ideals in these extensions. If we study abelian unramified extensions of $K$, one can prove that there exists a maximal field with this property. This result is an immediate consequence from Theorem 3.4.6 and Corollary 3.4.7, which will be treated later.

**Proposition 3.2.3.** *(Hilbert class field) Suppose $K$ is a number field. Then there is a unique extension $L$ of $K$ such that $L$ is an unramified abelian extension of $K$ and any unramified abelian extension $M$ of $K$ lies in $L$. This extension $L$ is called the* Hilbert class field *of $K$.*

The most important tool to determine whether primes split completely in the Hilbert class field (or any unramified abelian extension) is the Artin symbol. This is a unique element in the Galois group with certain properties. We can find it by noting that any element $\sigma \in \mathrm{Gal}(L/K)$ that leaves a prime $\mathfrak{P}$ lying over $\mathfrak{p}$ invariant, naturally induces an automorphism of the finite field $\mathcal{O}_L/\mathfrak{P}$, which is an element in the Galois group of the extension $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$.

Conversely, any automorphism in the Galois group of this extension of finite fields gives us a unique corresponding element in the Galois group $\mathrm{Gal}(L/K)$. If we take the Artin symbol to be the unique element corresponding to a generator of the Galois group of the extension of finite fields, better known as the Frobenius automorphism of the field, we get the following result. For a detailed proof, see [Cox13, Lemma 5.19, p. 95].

**Proposition 3.2.4.** *(Artin symbol) Let $K \subset L$ be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of $K$ which is unramified in $L$. If $\mathfrak{P}$ is a prime of $L$ lying over $\mathfrak{p}$, then there is a unique map $\sigma \in \mathrm{Gal}(L/K)$ that, for all $\alpha \in \mathcal{O}_L$, satisfies*

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

*This element $\sigma$ is called the* Artin symbol *of $\mathfrak{P}$ and is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$.*

We will now prove a few properties of the Artin symbol.

**Proposition 3.2.5.** *Let $K \subset L$ be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of $K$ that is unramified in $L$ and let $\mathfrak{P}$ be a prime of $L$ lying over $\mathfrak{p}$.*

1. *For any $\sigma \in \mathrm{Gal}(L/K)$ we have*
$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$
*Consequently for an abelian extension the Artin symbol only depends on the underlying prime $\mathfrak{p}$; we denote it by $\left(\frac{L/K}{\mathfrak{p}}\right)$ in this case.*
2. *The order of the Artin symbol of $\mathfrak{P}$ is the inertial degree $f$ of $\mathfrak{p}$ in $L$.*
3. *The prime $\mathfrak{p}$ splits completely in $L$ if and only if the Artin symbol of $\mathfrak{P}$ is the identity element.*

*Proof.* We will prove the statements individually.

1. Let $\sigma \in \mathrm{Gal}(L/K)$, then for any $\alpha \in \sigma(\mathfrak{P})$ we have $\sigma^{-1}(\alpha) \in \mathfrak{P}$ and thus
$$\left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}(\alpha) \equiv \sigma^{-1}(\alpha^{N(\mathfrak{p})}) \bmod \mathfrak{P}.$$
But this means we have
$$\sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$
and by uniqueness of the Artin symbol the result follows. For an abelian extension we can see, by noting that the Galois group acts transitively on the primes $\mathfrak{P}$ lying over $\mathfrak{p}$, that the Artin symbol depends solely on the underlying prime $\mathfrak{p}$.

2. The Artin symbol corresponds with the Frobenius automorphism in the Galois group of the finite extension
$\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$, which is of degree $f$. The Frobenius automorphism is a generator, and therefore is of order $f$. Consequently, the Artin symbol is of order $f$.

3. We have that the Artin symbol is the identity map if and only if its order is 1, which by statement 2. is equivalent to $f = 1$. But by assumption we have $e = 1$, and thus this condition is equivalent to $\mathfrak{p}$ splitting completely in $L$. □

**Example 3.2.6.** *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. The primes $3\mathbb{Z}$ and $5\mathbb{Z}$ are unramified in $\mathcal{O}_L$, since they do not divide $d_K = -4$. Now we find that the Artin symbols for these primes should satisfy*

$$\left(\frac{L/K}{3\mathbb{Z}}\right)(a+bi) \equiv (a+bi)^3 \bmod 3, \ \left(\frac{L/K}{5\mathbb{Z}}\right)(a+bi) \equiv (a+bi)^5 \bmod (2+i).$$

*By applying Fermat's little theorem, we find that*

$$(a+bi)^3 \equiv a^3 - b^3 i \equiv a - bi \bmod 3, \ (a+bi)^5 \equiv a^5 + b^5 i \equiv a + bi \bmod 5.$$

*Thus, for the prime $3\mathbb{Z}$ we see its Artin symbol is complex conjugation, while for the prime $5\mathbb{Z}$ it is the identity map. Indeed we see that the prime 5 splits completely in $L$, as we have $5\mathcal{O}_L = (2+i)\mathcal{O}_L(2-i)\mathcal{O}_L$.*

## 3.3 Orders in quadratic fields

In order to prove the Main Theorem on primes of the form $x^2 + ny^2$, we will study the behavior of primes in the ring $\mathbb{Z}[\sqrt{-n}]$. However, as we have seen in Example 3.1.3, this is not the full ring of integers of the field $K(\sqrt{-n})$ whenever $n \equiv 3 \bmod 4$ or $n$ is not squarefree. This more general case will be treated by showing that the ring $\mathbb{Z}[\sqrt{-n}]$ is an order.

**Definition 3.3.1.** *(Order) Let $K$ be a quadratic field. An* order *is a subring $\mathcal{O} \subset K$ containing $1 \in K$ such that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.*

We see that $\mathbb{Z}[\sqrt{-n}]$ is an order in $K = \mathbb{Q}(\sqrt{-n})$ for all positive integers $n$. We also see that the full ring of integers, as given in Example 3.1.3, is an order. More precisely, it is the *maximal order*, since any order $\mathcal{O}$ is contained in it. This follows by noting that, for any $\alpha \in \mathcal{O}$, by definition of an order we have $\alpha^2 = a\alpha + b$ for some integers $a, b$. Consequently, we find $\alpha \in \mathcal{O}_K$. Now, any order can be expressed in the form described in the following lemma.

**Lemma 3.3.2.** *Let $\mathcal{O} \subset K$ be an order in a quadratic field $K$. Then $\mathcal{O}$ has finite order in $\mathcal{O}_K$, and by setting $f = [\mathcal{O}_K : \mathcal{O}]$, we have*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K.$$

*Proof.* Since $\mathcal{O}$ and $\mathcal{O}_K$ are both finitely generated $\mathbb{Z}$-modules of the same rank, we find that $\mathcal{O}$ indeed has finite order in $\mathcal{O}_K$. Because we have $1 \in \mathcal{O}$, we find that $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. Since clearly $\mathbb{Z} + f\mathcal{O}_K$ is of rank $f$ in $\mathcal{O}_K$, we find that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. □

Now we can characterize any order by this number $f$. This leads to the following definition.

**Definition 3.3.3.** *(Conductor and discriminant) Let $K$ be a quadratic field and $\mathcal{O} \subset K$ an order. Set $f = [\mathcal{O}_K : \mathcal{O}]$, then we define $f$ to be the* conductor *of the order and $D = f^2 d_K$ to be the* discriminant *of the order.*

One can show that for any integral basis $(\alpha, \beta)$ of an order $\mathcal{O}$ in $K$, the discriminant is equal to $(\alpha\beta' - \alpha'\beta)^2$, where $\alpha \mapsto \alpha'$ is the nontrivial element of the group $\mathrm{Gal}(K/\mathbb{Q})$. This implies that the discriminant of $\mathbb{Z}[\sqrt{-n}]$ equals $-4n$, and we can thus easily compute the conductor of this order in the field $K = \mathbb{Q}(\sqrt{-n})$. An immediate consequence is that for any prime $p$ not dividing $n$, we find that $p$ does not divide $d_K$ and is thus unramified in $K$ by Proposition 3.1.11.

Let us study more closely the ideals of an order $\mathcal{O}$. In Corollary 3.1.6, we saw that for the maximal order $\mathcal{O}_K$ we have unique factorization of ideals. This property does not hold for orders in general. We will later see this property does hold for ideals which are prime to the conductor $f$ of the order, but first let us look into ideals in a more general context.

**Definition 3.3.4.** *(Fractional ideal) Let $K$ be a quadratic field and $\mathcal{O} \subset K$ an order. Let $\mathfrak{b} \subset \mathcal{O}$ be a subset. We say that $\mathfrak{b}$ is a* fractional ideal *if we have $\mathfrak{b} = \alpha\mathfrak{a}$ for some $\alpha \in K^*$ and $\mathfrak{a} \subset \mathcal{O}$ a non-zero ideal. A fractional ideal $\mathfrak{b}$ is called* proper *if we have $\mathcal{O} = \{\beta \in K \mid \beta\mathfrak{b} \subset \mathfrak{b}\}$, is called* invertible *if there is a fractional ideal $\mathfrak{d}$ such that $\mathfrak{b}\mathfrak{d} = \mathcal{O}$ and is called* principal *if $\mathfrak{b} = \beta\mathcal{O}$ for some $\beta \in K^*$.*

We can copy the proof of Proposition 3.1.5 to see that for an $\mathcal{O}$-ideal the quotient group $\mathcal{O}/\mathfrak{a}$ is finite. Therefore, we can define the norm in the same way, by setting $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. Now we define the ideal class group of an order $\mathcal{O}$.

**Proposition 3.3.5.** *Let $K$ be a quadratic field and $\mathcal{O} \subset K$ an order. Let $I(\mathcal{O})$ denote the set of proper fractional ideals of $\mathcal{O}$ and $P(\mathcal{O})$ the set of principal fractional ideals. Then $I(\mathcal{O})$ is a group under ideal multiplication and $P(\mathcal{O})$ is a subgroup of this group. Their quotient $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$ is called the* ideal class group *of the order $\mathcal{O}$.*

*Proof.* It is easy to show that a fractional ideal is proper if it is invertible. The opposite is also true, for a proof see [Cox13, Prop. 7.4, p. 122]. Now this means that each proper fractional ideal $\mathfrak{a}$ has an inverse $\mathfrak{a}^{-1}$. This means for any two proper fractional ideals $\mathfrak{a}, \mathfrak{b}$, we have that $(\mathfrak{a}\mathfrak{b})(\mathfrak{a}^{-1}\mathfrak{b}^{-1}) = \mathcal{O}$ and thus their product is invertible and hence proper. This proves that $I(\mathcal{O})$ is closed under ideal multiplication and thus forms a group. Since any principal fractional ideal $\beta\mathcal{O}$ for $\beta \in K^*$ is invertible, with inverse $\frac{1}{\beta}\mathcal{O}$, we find that $P(\mathcal{O})$ is contained in $I(\mathcal{O})$ and obviously closed under multiplication. □

The name ideal class group suggests that there is a relation with the form class group from section 2.4. This relation is described in the following theorem. A consequence is that one can show Dirichlet composition of forms indeed induces a well-defined group law on the equivalence classes of forms and thus proves Theorem 2.4.3. For a proof, see [Cox13, Thm. 7.7, p. 123].

**Theorem 3.3.6.** *Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive positive definite form of discriminant $D = -4n$. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field, and let $\mathcal{O}$ be the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. Then the ideal $[a, (-b + \sqrt{D})/2]$ is a proper ideal of $\mathcal{O}$, and the map sending $f(x, y)$ to this ideal induces an isomorphism between the form class group $C(D)$ and the ideal class group $C(\mathcal{O})$.*

One can also relate the ideal class group to the Galois group of abelian extension of the field $K$. But to do so, we must first relate the ideals of the order $\mathcal{O}$ to ideals of the maximal order $\mathcal{O}_K$. For this, we study the ideals of $\mathcal{O}$ which are prime to $f$, and we will find their ideal class group, obtained by taking the quotient of principal ideals generated by elements with norm prime to $f$, is naturally isomorphic to the ideal class group $\mathcal{O}$. Moreover, it is naturally isomorphic to a generalized ideal class group of the maximal order $\mathcal{O}_K$.

**Proposition 3.3.7.** *(Ideals prime to the conductor) Let $K$ be a quadratic field and let $\mathcal{O} \subset K$ be an order of conductor $f$. Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Then the following holds:*

1. *We have that $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$ if and only if $N(\mathfrak{a})$ is relatively prime to $f$. In case either of these conditions hold we say that $\mathfrak{a}$ is* prime to $f$.
2. *Any $\mathcal{O}$-ideal prime to $f$ is proper.*
3. *Let $I(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O})$ generated by all $\mathcal{O}$-ideals prime to $f$ and let $P(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O}, f)$ generated by the principal ideals of the form $\alpha\mathcal{O}$ with $\alpha \in \mathcal{O}$ such that $N(\alpha)$ is prime to $f$. Then the inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induces an isomorphism*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq C(\mathcal{O}).$$

*Proof.* We prove the statements individually.

1. Consider the map $\mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ induced by multiplication by $f$ on $\mathcal{O}$. Since $\mathcal{O}/\mathfrak{a}$ is isomorphic to $\mathbb{Z}/a\mathbb{Z}$, where $a = N(\mathfrak{a})$, by definition of the norm, we find that this map is an isomorphism if and only if $N(\mathfrak{a})$ is relatively prime to $f$. But one also sees, because the group is finite, the map is bijective if and only if it is surjective. Now this is equivalent to $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$, and the statement follows.
2. Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal prime to $f$. Suppose we have $\beta \in K$ such that $\beta\mathfrak{a} \subset \mathfrak{a}$. Now we have $1 \in \mathcal{O} = \mathfrak{a} + f\mathcal{O}$, so we can write $1 = \alpha + f \cdot \gamma$ with $\alpha \in \mathfrak{a}$ and $\gamma \in \mathcal{O}$. Now $\beta = \alpha\beta + f \cdot \gamma\beta$, where we have $\alpha\beta \in \mathfrak{a}$ by our assumption, and $f\gamma\beta \in f\mathcal{O}_K \subset \mathcal{O}$. Thus, we have $\beta \in \mathcal{O}$, and we find that $\mathfrak{a}$ is proper.
3. In Lemma 2.3.3, we saw that for each class in the form class group $C(D) \simeq C(\mathcal{O})$, there is an integer coprime to $D$ represented by a form in this class. One can show (see [Cox13, Thm. 7.7(iii), p. 124]) this implies that each class in $C(\mathcal{O})$ contains an ideal whose norm is prime to $D$ and thus prime to $f$. This means the induced map $I(\mathcal{O}, f) \to C(\mathcal{O})$ is surjective. By multiplicity properties of the norm function on ideals, one can show that the kernel of the map is $P(\mathcal{O}, f)$. For the full details, see [Cox13, Prop. 7.19, p. 130]. □

The next part will be relating ideals prime to $f$ to ideals of the maximal order. The next proposition will show every ideal prime to $f$ in $\mathcal{O}$ corresponds with a unique ideal prime to $f$ in $\mathcal{O}_K$. We denote the subgroup $I(\mathcal{O}_K, f)$ of ideals prime to $f$ in the maximal order by $I_K(f)$.

**Proposition 3.3.8.** *Let $K$ be a quadratic field and $\mathcal{O} \subset K$ an order of conductor $f$. Then the map given by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ is well defined and induces an isomorphism $I_K(f) \to I(\mathcal{O}, f)$ and has inverse map given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.*

*Proof.* Suppose that $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to $f$. Then we have an injection $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$. Now, since $\mathfrak{a}$ is prime to $f$, we have $\mathcal{O}_K = \mathfrak{a} + f\mathcal{O}_K$ and $f\mathcal{O}_K \subset \mathcal{O}$, so we see the map is also surjective. Therefore, we find that $N(\mathfrak{a} \cap \mathcal{O}) = N(\mathfrak{a})$. By Proposition 3.3.7, this immediately implies that both norms are relatively prime to $f$ and thus $\mathfrak{a} \cap \mathcal{O}$ is prime to $f$.

Suppose that $\mathfrak{b}$ is an $\mathcal{O}$-ideal prime to $f$. Then we have $1 \in \mathcal{O} = \mathfrak{b} + f\mathcal{O}$ and thus, for any $\alpha \in \mathcal{O}_K$, we find $\alpha \cdot 1 \in (\mathfrak{b} + f\mathcal{O})\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K + f\mathcal{O}_K$, so $\mathfrak{b}\mathcal{O}_K$ is prime to $f$.

The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ can be naturally extended to fractional ideals by mapping $\mathfrak{a}\mathfrak{b}^{-1}$ to $(\mathfrak{a} \cap \mathcal{O})(\mathfrak{b} \cap \mathcal{O})^{-1}$. The inverse map as given is obviously multiplicative and thus the only part left to prove is that it is indeed an inverse map. This follows from the identities $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$ for every $\mathcal{O}$-ideal $\mathfrak{a}$ prime to $f$ and $(\mathfrak{b} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{b}$ for every $\mathcal{O}_K$-ideal $\mathfrak{b}$ prime to $f$, which can be proven by noting that in each case one inclusion is clear, and the other can be proven using the ideals are prime to $f$ and the fact that $f\mathcal{O}_K \subset \mathcal{O}$. □

One can now deduce unique factorization of ideals in $\mathcal{O}$ prime to the conductor $f$ into prime ideals prime to $f$, by observing that this factorization is uniquely determined by the unique factorization of the corresponding ideal in $\mathcal{O}_K$ prime to $f$. From the isomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$, found in the proof op Proposition 3.3.8, it follows that, if $\mathfrak{a}$ is a prime ideal in $\mathcal{O}_K$ prime to $f$, then $\mathfrak{a} \cap \mathcal{O}$ is a prime ideal in $\mathcal{O}$ prime to $f$. This unique factorization, combined with class field theory, will be a key ingredient for proving the Main Theorem.

**Proposition 3.3.9.** *Let $K$ be an imaginary quadratic field. Let $\mathcal{O} \subset K$ be an order of conductor $f$. Let $P_{K,\mathbb{Z}}(f)$ be the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$ satisfying $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer $a \in \mathbb{Z}$ coprime to $f$. Then there are natural isomorphisms*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f).$$

*Proof.* The isomorphism $C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f)$ was proven in Proposition 3.3.7. The isomorphism $I(\mathcal{O}, f) \simeq I_K(f)$ from Proposition 3.3.8 induces a surjective map $I(\mathcal{O}, f) \to I_K(f)/P_{K,\mathbb{Z}}(f)$, so it remains to show the kernel of this map is the subgroup $P(\mathcal{O}, f)$.

By Lemma 3.3.2, we see that, for $\alpha \in \mathcal{O}_K$, the condition $\alpha \equiv a \bmod f\mathcal{O}_k$ with $a \in \mathbb{Z}$ implies $\alpha \in \mathcal{O}$. In the same manner, we can write $\alpha \equiv a \bmod f\mathcal{O}_K$ with $a \in \mathbb{Z}$ for any $\alpha \in \mathcal{O}$. Since $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ denotes the complex conjugate, we have

$$\alpha \equiv a \bmod f\mathcal{O}_K \iff N(\alpha) \equiv a^2 \bmod f\mathcal{O}_K.$$

Therefore, we find that the principal ideals $\alpha\mathcal{O}$ in the order $\mathcal{O}$ with $N(\alpha)$ prime to $f$ correspond exactly with the principal ideals $\alpha\mathcal{O}_K$ in $\mathcal{O}_K$ with $\alpha \equiv a \bmod f\mathcal{O}_K$ for some $a \in \mathbb{Z}$ coprime to $f$. □

## 3.4 Theorems of class field theory

The Artin symbol from section 3.1.2 allows us to relate prime ideals in $K$ unramified in an abelian extension $L$ of $K$ to the Galois group of this extension. In Proposition 3.2.5, we saw that the primes that split completely in this extension are exactly the primes having Artin symbol $1 \in \mathrm{Gal}(L/K)$. In this section, we will use unique factorization of ideals into prime ideals to introduce a map $C(\mathcal{O}) \to \mathrm{Gal}(L/K)$, which will be called the Artin map. Since for any element $\sigma \in \mathrm{Gal}(L/K)$ there is a prime ideal with Artin symbol $\sigma$, this map is an isomorphism.

The first theorem of class field theory will show that the Galois group of any abelian extension $L$ of $K$ corresponds with some generalized ideal class group. However, it is the existence theorem, which tells us that any generalized ideal class group corresponds with a unique abelian extension $L$ of $K$, that will be crucial for the proof of the Main Theorem.

### 3.4.1 Moduli

We first introduce moduli, which allow us to define the Artin map for any extension, where the primes that ramify are determined by the modulus. In this way we can ensure we obtain an extension in which all relevant primes are unramified, and thus have a corresponding Artin symbol.

**Definition 3.4.1.** *(Modulus) Let $K$ be a number field. We define a* modulus $\mathfrak{a}$ *to be a formal product over all primes $\mathfrak{p}$, both finite and real infinite, with non-negative exponents $n_\mathfrak{p}$, of which only finitely many are non-zero and are equal to 0 or 1 for all infinite primes.*

The condition on the exponents imply that any modulus can be written as the formal product of an $\mathcal{O}_K$-ideal $\mathfrak{m}_0$ and a product of distinct real primes $\mathfrak{m}_\infty$. In case of an imaginary quadratic field, this means that a modulus can be regarded as an ideal. We say a modulus *divides* another modulus whenever all of its exponents are equal or smaller. The modulus with exponents all equal to zero, which can be regarded as the ideal $\mathcal{O}_K$, is denoted by 1.

Now we can define the $I_K(\mathfrak{m})$ as the subgroup of $I_K$ generated by all the ideals prime to $\mathfrak{m}_0$ and $P_{K,1}(\mathfrak{m})$ as the subgroup generated by the principal ideals $\alpha\mathcal{O}_K$ prime to $\mathfrak{m}_0$ with $\alpha \in \mathcal{O}_K$ satisfying $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all real infinite primes $\sigma$ dividing $\mathfrak{m}$, i.e. the primes with exponent 1.

**Definition 3.4.2.** *(Congruence subgroup) Let $K$ be a number field and $\mathfrak{m}$ a modulus. A subgroup $H \subset I_K(\mathfrak{m})$ containing $P_{K,1}(\mathfrak{m})$ is called a* congruence subgroup *for $\mathfrak{m}$. The corresponding quotient group $I_K(\mathfrak{m})/H$ is called a* generalized ideal class group *for $\mathfrak{m}$.*

Now if we look at an order of an imaginary quadratic field and its conductor $f$, we see that the group $I_K(f)$ from section 3.3 is equal to the group $I_K(\mathfrak{m})$, where $\mathfrak{m}$ is the modulus $f\mathcal{O}_K$. The group $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for $\mathfrak{m} = f\mathcal{O}_K$, and by Proposition 3.3.9, the class group $C(\mathcal{O})$ is a generalized ideal class group for $\mathfrak{m}$.

**Definition 3.4.3.** *(Artin map) Let $K$ be a number field and $K \subset L$ an abelian extension of $K$. Let $\mathfrak{m}$ be a modulus such that all primes of $K$ that ramify in $L$ divide $\mathfrak{m}$. Define homomorphism $\Phi_{L/K,\mathfrak{m}}$ by*

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K),\ \mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}}\right),$$

*where $\left(\frac{L/K}{\mathfrak{a}}\right)$ is obtained from the unique factorization of $\mathfrak{a}$ into prime ideals not dividing $\mathfrak{m}$. This map $\Phi_{L/K,\mathfrak{m}}$ is called the* Artin map *for $K \subset L$ and $\mathfrak{m}$.*

The following theorem, which is known as the Artin reciprocity theorem, describes a relation between abelian extensions and congruence subgroups. A proof can be found in [Jan96, Ch. V, Thm. 5.8, p. 197].

**Theorem 3.4.4.** *(Artin reciprocity theorem) Let $K \subset L$ be an abelian extension of number fields and let $\mathfrak{m}$ be a modulus such that any prime of $K$ that ramifies in $L$ divides it. Then the Artin map $\Phi_{L/K,\mathfrak{m}}$ is surjective. If the primes dividing $\mathfrak{m}$ have sufficiently large exponents, then $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$.*

This theorem says that for any abelian extension $K \subset L$ and modulus $\mathfrak{m}$ divisible by all primes of $K$ that ramify in $L$, with sufficiently large exponents, the kernel of the Artin map is a congruence subgroup for $\mathfrak{m}$ and so $\mathrm{Gal}(L/K)$ is naturally isomorphic to a generalized ideal class group for this modulus. It is clear though that for any modulus divisible by $\mathfrak{m}$, we have that the kernel of the Artin map is a congruence subgroup as well. The next theorem will tell us there is a modulus which is in the obvious sense the smallest modulus. For a proof, see [Jan96, Ch. V, §6 and Thm. 11.11].

**Theorem 3.4.5.** *(Conductor theorem) Let $K \subset L$ be an abelian extension of number fields. Then there is a modulus $\mathfrak{f}$ such that a prime of $K$ ramifies in $L$ if and only if it divides this modulus. Furthermore, for any modulus $\mathfrak{m}$ divisible by all primes of $K$ that ramify in $L$ we have that $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup if and only if $\mathfrak{f}$ divides $\mathfrak{m}$.*

*This modulus $\mathfrak{f}$ is denoted by $\mathfrak{f}(L/K)$ and is called the* conductor *of the extension.*

Hence, we see that, for any abelian extension of a number field $K \subset L$, there is a corresponding modulus $\mathfrak{m}$ divisible by all primes ramifying such that the Galois group $\mathrm{Gal}(L/K)$ is naturally isomorphic to a generalized ideal class group for this modulus. The next theorem asserts the opposite statement, which says that for any generalized ideal class group there is a corresponding abelian extension. The proof can be found in [Jan96, Ch. V, Thm. 9.9, p. 215].

**Theorem 3.4.6.** *(Existence theorem) Let $K$ be a number field, let $\mathfrak{m}$ be a modulus of $K$ and let $H$ be a congruence subgroup for $\mathfrak{m}$. Then there is a unique abelian extension $K \subset L$, such that any prime of $K$ that ramifies in $L$ divides $\mathfrak{m}$, and for the Artin map $\Phi_{L/K,\mathfrak{m}}$ we have*

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

The following corollary shows that there is an inclusion-reversing relation between abelian extensions of $K$ and congruence subgroups of a modulus $\mathfrak{m}$.

**Corollary 3.4.7.** *Let $K$ be a number field and let $L, M$ be abelian extension of $K$. Then we have $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all primes of $K$ ramified in either $L$ or $M$, for which $\ker(\Phi_{L/K,\mathfrak{m}})$ and $\ker(\Phi_{M/K,\mathfrak{m}})$ are congruence subgroups for $\mathfrak{m}$, such that*

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

*Proof.* Suppose we have $L \subset M$. By Theorem 3.4.4, there are moduli such that the kernels of their respective Artin maps are congruence subgroups. The product of this moduli is a modulus $\mathfrak{m}$, such that both kernels of the Artin maps with modulus $\mathfrak{m}$ are congruence subgroups for $\mathfrak{m}$. Now for any prime $\mathfrak{p}$ of $K$, consider the restriction of the Artin symbol $\left(\frac{M/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(M/K)$ to $L$. By uniqueness of the Artin symbol (Proposition 3.2.4), this is the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$. Thus we find $\ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$.

Now suppose that there is a modulus $\mathfrak{m}$ divisible by all primes of $K$ ramified in either $L$ or $M$, such that $\ker(\Phi_{L/K,\mathfrak{m}})$ and $\ker(\Phi_{M/K,\mathfrak{m}})$ are congruence subgroups for $\mathfrak{m}$ with $\ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$. Consider the subgroup $H \subset \mathrm{Gal}(L/K)$, which is the image under the Artin map $\Phi_{M/K,\mathfrak{m}}$ of the subgroup $\ker(\Phi_{L/K,\mathfrak{m}})$. By Galois theory, there is a field $K \subset N \subset M$ corresponding to this subgroup. For the modulus $\mathfrak{m}$, the corresponding congruence subgroup $\ker(\Phi_{N/K,\mathfrak{m}})$ contains $\ker(\Phi_{M/K,\mathfrak{m}})$ by the first part of this proof. Since there is a unique subgroup of $I_K(\mathfrak{m})$ containing $\ker(\Phi_{M/K,\mathfrak{m}})$ that maps to $H$ under the Artin map $\Phi_{M/K,\mathfrak{m}}$, we have $\ker(\Phi_{L/K,\mathfrak{m}}) = \ker(\Phi_{N/K,\mathfrak{m}})$. Finally, Theorem 3.4.6 implies that $N = L$ and thus we find $L \subset M$. □

**Remark 3.4.8.** *Proposition 3.2.3, which ensured the existence of the Hilbert class field, is an immediate consequence of Theorem 3.4.6 and Corollary 3.4.7, by applying the results to the modulus $\mathfrak{m} = 1$, so that $P_{K,1}(\mathfrak{m}) = P_K$. If we define the Hilbert class field of $K$ to be the unique abelian extension in Theorem 3.4.6 corresponding with the congruence subgroup $P_K \subset I_K$, it is clearly unramified. For any unramified abelian extension $M$ of $K$, the kernel of the corresponding Artin map is a congruence subgroup by Theorem 3.4.5. This means it contains $P_K$, and by Corollary 3.4.7 we find that $M$ is contained in the Hilbert class field.*

### 3.4.2 Reciprocity laws

In Chapter 1, we discussed several reciprocity laws for rings of integers. While these results relied on unique factorization of integers, which does not hold in general extensions, these laws can be generalized to the level of ideals. For this, we first define the Legendre symbol in a more general context. Where previously these symbols were defined in terms of elements, we now define them in terms of ideals. First, let $K$ be a number field containing a primitive $n$-th root of unity $\zeta_n$. Then, for any prime ideal $\mathfrak{p}$ coprime to $n$, it is clear that $x^n - 1$ is separable modulo $\mathfrak{p}$, and thus the classes of $\zeta_n^k$ for $0 \leq k \leq n-1$ in $\mathcal{O}_K/\mathfrak{p}$ are its $n$ distinct roots. By applying Fermat's Little Theorem to $\zeta_n$, one immediately finds that $n \mid N(\mathfrak{p}) - 1$.

Now let $\alpha \in \mathcal{O}_K$ be prime to $\mathfrak{p}$. Then, we have that $\alpha^{(N(\mathfrak{p})-1)/n}$ is a root of $x^n - 1$ modulo $\mathfrak{p}$, and therefore congruent to a unique $n$-th root of unity. This will be defined as the $n$-th Legendre symbol of $\alpha$.

**Definition 3.4.9.** *(Legendre symbol) Let $K$ be a number field containing a primitive $n$-th root of unity. Let $\mathfrak{p}$ be a prime of $K$ prime to $n$ and let $\alpha \in \mathcal{O}_K$ be prime to $\mathfrak{p}$. Then the* $n$th Legendre symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ *of $\alpha$ is defined to be the unique $n$th root of unity satisfying*

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \mod \mathfrak{p}.$$

For any prime $\mathfrak{p}$ of $K$ prime to $n$ and $\alpha$, the corresponding $n$th Legendre symbol of $\alpha$ is now defined. By unique factorization of ideals, we can extend this to define the $n$th Legendre symbol of $\alpha$ for any ideal $\mathfrak{a} \in I_K(n\alpha)$, where $I_K(n\alpha)$ is the set generated by primes not containing $n\alpha$. More generally, we can define it for $\mathfrak{a} \in I_K(\mathfrak{m})$, where $\mathfrak{m}$ is a modulus divisible by all primes containing $n\alpha$. This yields a map $I_K(\mathfrak{m})$ to the group $\mu_n$ of $n$-th roots of unity in $\mathbb{C}$, denoted by $\left(\frac{\alpha}{\cdot}\right)_n$. Now if we consider the extension $K \subset L = K(\sqrt[n]{\alpha})$ of $K$, Galois theory shows that any $\sigma \in \mathrm{Gal}(L/K)$ acts on $\sqrt[n]{\alpha}$ by multiplying it with some $n$-th root of unity. Now, by associating each element in the Galois group to this root of unity, we obtain an injective homomorphism $\mathrm{Gal}(L/K) \to \mu_n$, which we denote by $i_n$. Weak reciprocity says that the composition of this map with the Artin map is exactly the map $I_K(\mathfrak{m}) \to \mu_n$ given by the Legendre symbol whenever $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup.

**Theorem 3.4.10.** *(Weak reciprocity) Let $K$ be a number field containing a primitive $n$-th root of unity $\zeta_n$. Let $\alpha \in \mathcal{O}_K \setminus \{0\}$ and let $L = K(\sqrt[n]{\alpha})$. Let $\mathfrak{m}$ be a modulus such that any prime containing $n\alpha$ divides $\mathfrak{m}$ and such that $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup. Then*

$$\left(\frac{\alpha}{\cdot}\right)_n = i_n \circ \Phi_{L/K,\mathfrak{m}}.$$

*Proof.* By definition, for any prime $\mathfrak{p} \in I_K(\mathfrak{m})$, we have that $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ is the unique $n$-th root of unity congruent to $\alpha^{(N(\mathfrak{p})-1)/n}$ modulo $\mathfrak{p}$. However, by definition of the Artin symbol, we have that

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{N(\mathfrak{p})-1} \equiv \alpha^{(N(\mathfrak{p})-1)/n} \bmod \mathfrak{P},$$

for any prime $\mathfrak{P}$ in $L$ lying over $\mathfrak{p}$. Consequently, we see the Artin symbol maps to the Legendre symbol under $i_n$ and, by unique factorization into primes, the theorem follows. □

It is possible to prove Theorem 1.1.4 using weak reciprocity, by considering the field $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}$, which is contained in $\mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi i/p}$ denotes a $p$-th root of unity. This fact ensures that $\ker(\Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q},p\infty})$ is a congruence subgroup for the modulus $p\infty$, where $\infty$ denotes the real infinite prime of $\mathbb{Q}$. Then, the generalized Legendre symbol from Theorem 3.4.10 can be shown to equal the Legendre symbol $\left(\frac{\cdot}{p}\right)$, and the quadratic reciprocity law follows.

Another theorem, known as strong reciprocity, describes a direct relation between the Legendre symbols of two relatively prime elements $\alpha, \beta \in \mathcal{O}_K$. This theorem can be used to prove the cubic and biquadratic reciprocity from Theorem 1.2.3.

### 3.4.3 Čebotarev density theorem

In this section, we will the Dirichlet density of sets of prime ideals in a number field, and relate these sets to abelian extensions of the number field; or more specifically the kernel of the Artin maps of these extensions. The results found will be used in the proof of the Main Theorem, in order to prove the uniqueness of the polynomial $f_n(x)$.

To do so, we define the Dirichlet density of a set of primes and then we list some properties of this density. To prove these properties, we first introduce the Dedekind $\zeta$-function. For a number field $K$, denote by $\mathcal{P}_K$ the set of all prime ideals of $\mathcal{O}_K$.

**Definition 3.4.11.** *(Dirichlet $\zeta$-function) Let $K$ be a number field. Then the* Dirichlet $\zeta$-function $\zeta_K(s)$ *of $K$ is defined as*

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} N(\mathfrak{a})^{-s},$$

*where the sum is over all ideals $\mathfrak{a} \subset \mathcal{O}_K$.*

We now list a few important properties of this function, which are proven in [Neu86, Ch. V, Thm. 2.2, p. 117].

**Proposition 3.4.12.** *Let $K$ be a number field and let $\zeta_K(s)$ be the Dirichlet $\zeta$-function of $K$. Then the following statements hold.*

1. *The series $\zeta_K(s)$ converges absolutely for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$.*
2. *The function $\zeta_K(s)$ has an analytic continuation to some open set containing $\{s \in \mathbb{C} \mid \operatorname{Re} s > 1\} \setminus \{1\}$, which has a simple pole at $s = 1$.*
3. *For all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$, we have the identity*

$$\prod_{\mathfrak{p} \in \mathcal{P}_K} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

Now we can define the Dirichlet density of a set of primes.

**Definition 3.4.13.** *(Dirichlet density) Let $K$ be a number field and let $\mathcal{S} \subset \mathcal{P}_K$ be a set of primes of $K$. Then the* Dirichlet density $\delta(\mathcal{S})$ *of the set $\mathcal{S}$ is defined to be*

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

*whenever the limit exists; else we say the density is undefined.*

**Proposition 3.4.14.** *Let $K$ be a number field and let $\mathcal{S}, \mathcal{T} \subset \mathcal{P}_K$ be sets of primes of $K$. Assume $\delta(\mathcal{S})$ and $\delta(\mathcal{T})$ are defined. Then the following statements hold.*

1. *We have $\delta(\mathcal{P}_K) = 1$.*
2. *If $\mathcal{S} \subset \mathcal{T}$, then $\delta(\mathcal{S}) \leq \delta(\mathcal{T})$.*
3. *We have $0 \leq \delta(S) \leq 1$.*
4. *If $\mathcal{S}$ is finite, then $\delta(\mathcal{S}) = 0$.*
5. *If the intersection $\mathcal{S} \cap \mathcal{T}$ is finite, then $\delta(\mathcal{S} \cup \mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T})$.*
6. *If the difference $\mathcal{S} \triangle \mathcal{T}$ is finite, then $\delta(\mathcal{S}) = \delta(\mathcal{T})$.*

*Proof.* We prove the statement individually. Note that statement 1. in Proposition 3.4.12 implies that $\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}$ is bounded for $s > 1$.

1. This statement follows from the identity
$$\delta(\mathcal{P}_K) = \lim_{s \to 1^+} \frac{\log(\zeta_K(s))}{-\log(s-1)} = 1.$$
See [Jan96, Ch. VI, Thm. 4.6, p. 159] for a proof of this identity.
2. For $\mathcal{S} \subset \mathcal{T}$, we have $\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s} \leq \sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}$ for $s > 1$, which implies that the same inequality holds for their densities.
3. Since $\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}$ is positive for $s > 1$ whenever $\mathcal{S}$ is non-empty, we find that $\delta(\mathcal{S}) \geq 0$. Now we have $\mathcal{S} \subset \mathcal{P}_K$, so statement 1. and 2. imply $\delta(\mathcal{S}) \leq 1$.
4. This is an immediate consequence from the fact that in this case the sum $\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-1}$ is finite.
5. The equality is clear for disjoint sets $\mathcal{S}$ and $\mathcal{T}$. Combining this with statement 4. shows the result still holds whenever the intersection is finite.
6. It follows as an immediate consequence of statement 4. □

The most important property of the density for us, is its relation to primes in number fields, or more specifically Galois extensions of number fields. This relation is described in the next theorem, which has a proof that can be found in [Neu86, Ch. V, Thm. 6.4, p. 132].

**Theorem 3.4.15.** *(Čebotarev density theorem) Let $K \subset L$ be a Galois extension of number fields and let $\sigma \in \mathrm{Gal}(L/K)$. Let $C_\sigma$ be the conjugacy class of $\sigma$ in $\mathrm{Gal}(L/K)$. Let $\mathcal{S} \subset \mathcal{P}_K$ be the set of primes $\mathfrak{p}$ unramified in $L$, such that there is some prime $\mathfrak{P}$ in $L$ lying over $\mathfrak{p}$ with Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right) \in C_\sigma$. Then we have*
$$\delta(\mathcal{S}) = \frac{|C_\sigma|}{[L:K]}.$$

Our main interest is abelian extensions, and we see that Theorem 3.4.15 gives a more precise result for these kind of extensions. We have that $C_\sigma = \{\sigma\}$ for all $\sigma \in \mathrm{Gal}(L/K)$ in this case. This means that for any $\sigma \in \mathrm{Gal}(L/K)$, the set $\mathcal{S}$ of primes $\mathfrak{p}$ in $K$ unramified in $L$ with Artin symbol $\sigma$, the density is $\delta(\mathcal{S}) = 1/[L:K]$. Note also that this immediately proves surjectivity of the Artin map.

We will now apply Theorem 3.4.15, that relates inclusion of fields to inclusion of sets of primes that split completely in an extension. For this, we first introduce some additional notation. We denote by $\mathcal{S}_{L/K} \subset \mathcal{P}_K$ the set of primes $\mathfrak{p}$ in $K$ that split completely in a finite extension $L$ of $K$. Also, denote by $\tilde{\mathcal{S}}_{L/K} \subset \mathcal{P}_K$ the set of primes $\mathfrak{p}$ in $K$ unramified in $M$, for which there is a prime $\mathfrak{P}$ in $M$ lying over $\mathfrak{p}$ so that the inertial degree $f_{\mathfrak{P}|\mathfrak{p}}$ of $\mathfrak{P}$ over $\mathfrak{p}$ is equal to 1.

For two subsets $\mathcal{S}, \mathcal{T} \subset \mathcal{P}_K$, we write $\mathcal{T} \dot{\subset} \mathcal{S}$ whenever $\mathcal{T} \setminus \mathcal{S}$ is finite, and we write $\mathcal{T} \doteq \mathcal{S}$ whenever $\mathcal{T} \triangle \mathcal{S}$ is finite.

**Theorem 3.4.16.** *Let $K$ be a number fields and let $L, M$ be finite extensions of $K$. Then the following statements hold.*

1. *If $L$ is Galois over $K$, then*
$$L \subset M \iff \tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}.$$
2. *If $M$ is Galois over $K$, then*
$$L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}.$$

*Proof.* Let us consider the first statement. The implication to the right is clear. Let $N$ be a Galois extension of $K$, which contains both $L$ and $M$. Let $\sigma \in \mathrm{Gal}(N/M)$. By Theorem 3.4.15, there is a prime $\mathfrak{p}$ in $K$ unramified in $N$, such that there is a prime $\mathfrak{P}$ in $N$ lying over $\mathfrak{p}$, which has Artin symbol $\left(\frac{N/K}{\mathfrak{P}}\right)$ that lies in the conjugacy class of $\sigma$. By Proposition 3.2.5 each conjugate is also the Artin symbol of some prime lying over $\mathfrak{p}$, thus we may assume that we have
$$\left(\frac{N/K}{\mathfrak{P}}\right) = \sigma.$$

Since $\mathfrak{p}$ is unramified in $N$, we see that $\mathfrak{p}$ is also unramified in $M$. For any $\alpha \in \mathcal{O}_M$ we have $\sigma(\alpha) = \alpha$, since $\sigma \in \mathrm{Gal}(N/M)$. But $\sigma = \left(\frac{N/K}{\mathfrak{P}}\right)$ being the Artin symbol of $\mathfrak{P}$ over $\mathfrak{p}$ implies that $\sigma\big|_M$ is the Artin symbol $\left(\frac{M/K}{\mathfrak{P}'}\right)$ of $\mathfrak{P}' = \mathcal{O}_M \cap \mathfrak{P}$ over $\mathfrak{p}$. Now $N(\mathfrak{p}) = N(\mathfrak{P}')$ immediately follows, so we find that $f_{\mathfrak{P}'|\mathfrak{p}} = 1$ and consequently $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K} \subset \mathcal{S}_{L/K}$.

This means $\mathfrak{p}$ splits completely in $L$, and consequently, by Proposition 3.2.5, we have $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. But $\sigma = \left(\frac{N/K}{\mathfrak{P}}\right)$ being the Artin symbol of $\mathfrak{P}$ over $\mathfrak{p}$ implies that $\sigma\big|_L$ is the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$, from which follows that
$$\sigma\big|_L = \left(\frac{L/K}{\mathfrak{p}}\right) = 1.$$
Then $\sigma \in \mathrm{Gal}(N/L)$ follows, and therefore we conclude $\mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/L)$. Thus, we find that $L \subset M$.

Now for the second statement, note again that the implication to the right is clear. For a prime $\mathfrak{p}$ of $K$, it can be shown that $\mathfrak{p}$ splits completely in $L$ if and only if it splits completely in the normal closure $L'$ of $K$ (see [Mar77, Cor. to Thm. 31, p. 108]). So we find that $\mathcal{S}_{L/K} = \mathcal{S}_{L'/K}$ and, since $M$ is Galois over $K$, we find that $\mathcal{S}_{M/K} = \tilde{\mathcal{S}}_{M/K}$. Thus we find that $\mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ is equivalent to $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L'/K}$, which by the first statement is equivalent to $L' \subset M$. But this immediately implies $L \subset M$. □

# Chapter 4

# Main Theorem

The theorems of class field theory from chapter 3 allow us to prove the Main Theorem. To do so, we first define the ring class field of an order $\mathbb{Z}[\sqrt{-n}]$, and then show that an odd prime $p$ not dividing $n$ is of the form $x^2 + ny^2$ if and only if it splits completely in $L$. Then we describe the field $L$ by finding a monic integer polynomial $f_n(x)$, which will be the minimal polynomial of a primitive element of the extension $K = \mathbb{Q}(\sqrt{-n}) \subset L$ and prove the equivalence in the Main Theorem for this polynomial.

In the second part of the proof, we show that any polynomial of the given form satisfying the equivalence is the minimal polynomial of some primitive element of this extension. Finally, we work out an example to illustrate the use of the theorem.

## 4.1 Ring class field

If we look at the behavior of a prime $p$ in the ring $\mathbb{Z}[\sqrt{-n}]$, we see that a prime is of the form $x^2 + ny^2$ when it splits into two principal ideals $(x+\sqrt{-n}y)(x-\sqrt{-n}y)$ in this ring. The principal ideals in this ring we are interested in, is the group $P_{K,\mathbb{Z}}(f)$ of principal ideals prime to the conductor $f$. This group is a generalized ideal class group of $K$ for the modulus $f\mathcal{O}_K$, and thus corresponds with a unique abelian extension, which will be called the ring class field.

**Definition 4.1.1.** *(Ring class field) Let $\mathcal{O} \subset K$ be an order in an imaginary quadratic field. Then the unique abelian extension $L$ from Theorem 3.4.6, corresponding with the congruence subgroup $P_{K,\mathbb{Z}}(f)$ for the modulus $f\mathcal{O}_K$, is called the* ring class field *of the order $\mathcal{O}$. For this field, we have that all primes of $K$ ramified in $L$ divide the modulus $f\mathcal{O}_K$, and the Artin map induces an isomorphism*

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

**Remark 4.1.2.** *In case we have that the ring of integers of a number fields is given by $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$, which happens whenever $n$ is squarefree and $n \not\equiv 3 \bmod 4$, we find that the conductor equals 1. In this case, we have $I_K(1) = I_K$ and $P_{K,\mathbb{Z}}(1) = P_{K,1}(1) = P_K$, so the ring class field is equal to the Hilbert class field, as seen in Remark 3.4.8.*

For us, the most important property of the ring class field is given by the following theorem.

**Theorem 4.1.3.** *Let $n$ be a positive integer. Let $L$ be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the field $K = \mathbb{Q}(\sqrt{-n})$. Then $L$ is Galois over $\mathbb{Q}$, and if $p$ is an odd prime not dividing $n$, then*

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

*Proof.* Let $f$ be the conductor of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ and let $\mathfrak{m} = f\mathcal{O}_K$ be the corresponding modulus. Now let $\tau$ denote complex conjugation. Then for any prime $\mathfrak{p}$ in $K$ unramified in $\tau(L)$, we see that $\mathfrak{p}$ is a prime of $K$ unramified in $\tau(L)$, and we have $\left(\frac{\tau(L)/K}{\mathfrak{p}}\right) = \tau\left(\frac{L/K}{\tau(\mathfrak{p})}\right)\tau$. Therefore, we find that

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

Because $L$ is the ring class field of $K$, we have $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f)$. Now we have $\tau(f\mathcal{O}_K) = f\mathcal{O}_K$, which shows that if $\alpha \equiv a \bmod f\mathcal{O}_K$ for $a \in \mathbb{Z}$, then also $\tau(\alpha) \equiv a \bmod f\mathcal{O}_K$. So we can conclude that $\tau(P_{K,\mathbb{Z}})(f) = P_{K,\mathbb{Z}}(f)$, and consequently we have $\ker(\Phi_{L/K,\mathfrak{m}}) = \ker(\Phi_{\tau(L)/K,\mathfrak{m}})$. By Corollary 3.4.7, this implies that $\tau(L) = L$.

Let $\beta \in L$ and let $f(x) \in K[X]$ be its minimal polynomial over $K$. Then $g(x) = f(x)\tau(f(x))$ is a polynomial with coefficients in $\mathbb{Q}$, so the minimal polynomial of $\beta$ over $\mathbb{Q}$ divides $g(x)$. Since $f(x)$ splits in $L$ and $\tau(L) = L$, we find that $g(x)$ splits in $L$, and thus the minimal polynomial of $\alpha$ over $\mathbb{Q}$ splits in $L$. Thus, we see that $L$ is Galois over $\mathbb{Q}$.

We know the order $\mathcal{O}$ has discriminant $-4n = f^2 d_K$, and since $p$ is an odd prime not dividing $n$, this means that $p$ does not divide $d_K$ and therefore is unramified in $K$. Now $p = x^2 + ny^2$ implies that we can write $p = (x + y\sqrt{-n})(x - y\sqrt{-n})$, so that $p\mathcal{O}_K$ can be written as a product of two distinct principal ideals with generators in $\mathcal{O}$. Conversely, if $p\mathcal{O}_K$ is the product of two distinct principal ideals with generators in $\mathcal{O}$, we know that one of these ideals can be written as $(x + \sqrt{-ny})\mathcal{O}_K$ for some integers $x, y \in \mathbb{Z}$. Then, by noting the Galois group acts transitively on the primes, the second ideal will be $(x - \sqrt{-ny})\mathcal{O}_K$, and we find $p = x^2 + ny^2$. So, we see that

$$p = x^2 + ny^2 \iff p\mathcal{O}_K \text{ is the product of two distinct ideals of the form } \mathfrak{p} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O}.$$

Since $p$ does not divide $-4n = f^2 d_K$, we find that it does not divide $f$. Thus, we see that the algebraic integer $\alpha$ in above equivalence is necessarily congruent modulo $f\mathcal{O}_K$ to an integer $a$ prime to $f$, while at the same time for any $\alpha \in \mathcal{O}_K$ congruent to an integer $a$ modulo $f\mathcal{O}_K$ we have that $\alpha \in \mathcal{O}$. This means that a prime ideal $\mathfrak{p}$ dividing $p$ is of the form $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}$ if and only if $\mathfrak{p} \in P_{K,\mathbb{Z}}(f)$. Since this is the kernel of the Artin map by construction of the ring class field, this condition is equivalent to $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. By Proposition 3.2.5, we now find

$$p\mathcal{O}_K \text{ is the product of two distinct ideals of the form } \mathfrak{p} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O} \iff p \text{ splits completely in } L.$$

Finally, combining the two equivalences above completes the proof. □

## 4.2 Primes of the form $x^2 + ny^2$

In this subsection, we give a proof of the Main Theorem for the representation of primes by the form $x^2+ny^2$, which gives a complete description when a prime can be expressed by this form for any positive value of $n$. Then we work out the example where $n = 15$, and finally, we discuss some limitations of the theorem.

### 4.2.1 Proof of the Main Theorem

**Theorem 4.2.1.** *(Main Theorem) Let $n$ be a positive integer. Then there is a polynomial $f_n(x) \in \mathbb{Z}[X]$ which is monic and irreducible and has degree $h(-4n)$, such that, for any odd prime $p$ not dividing $n$ or the discriminant of $f_n(x)$, we have*

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

*Furthermore, a monic integer polynomial $f_n(x)$ of degree $h(-4n)$ satisfies above condition if and only if $f_n(x)$ is irreducible over $\mathbb{Z}$, and is the minimal polynomial of a real algebraic integer $\alpha$, for which we have $L = K(\alpha)$, where $K = \mathbb{Q}(\sqrt{-n})$ and $L$ is the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in $K$.*

*Proof.* Suppose we have an odd prime $p$ not dividing $n$. Then, by Theorem 4.1.3, we see that $p = x^2 + ny^2$ if and only if $p$ splits completely in the ring class field $L$ of the order $\mathbb{Z}[\sqrt{-n}]$. Since $L$ is Galois over $\mathbb{Q}$ by Theorem 4.1.3, we see that $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$, as $L \cap \mathbb{R}$ is fixed by complex conjugation, which is in $\mathrm{Gal}(L/\mathbb{Q})$. Now for any $\alpha \in L \cap \mathbb{R}$, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K(\alpha) : K] = [K(\alpha) : \mathbb{Q}]/2$. So, for $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ such that $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$, we find that $L = K(\alpha)$. Therefore, we may assume that $L = K(\alpha)$ for some real algebraic integer $\alpha$.

Let $f_n(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$ over $K$, which has integer coefficients, because $\alpha$ is real. Because of the isomorphisms $C(-4n) \simeq C(\mathcal{O}) \simeq \mathrm{Gal}(L/K)$, we find that the degree of $f_n(x)$ is $[L : K] = h(\mathcal{O}) = h(-4n)$. By Theorem 3.1.8, we can see a prime $p$ splits completely in $L$ if and only if it splits completely in $K$ and some prime $\mathfrak{p}$ of $K$ lying over $p$ splits completely in $L$. By Proposition 3.1.10, we see that, for $p$ not dividing $n$ or the discriminant of $f_n(x)$, this is equivalent to $x^2 + n \equiv 0 \bmod p$ and $f_n(x) \equiv 0 \bmod \mathfrak{p}$ both having a solution in their respective ring of integers, as both polynomials are separable modulo $p$. As $p$ splits completely in $K$, we have $f = 1$ for this extension, which implies $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$. we find that $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$ and $f_n(x) \equiv 0 \bmod p$ has an integer solution.

Turning to the last part of the theorem, let $f_n(x)$ be a monic integer polynomial of degree $h(-4n)$ satisfying the equivalence in the Main Theorem. Let $\alpha$ be a root of $f_n(x)$ and set $M = K(\alpha)$. Then we have $\alpha \in \mathcal{O}_M$, since $f_n(x)$ has integer coefficients. Now consider a prime $p$ such that $p \in \tilde{\mathcal{S}}_{M/\mathbb{Q}}$. Let $\mathfrak{P}$ be a prime in $M$ such that $f_{\mathfrak{P}|p} = 1$, then clearly for the prime $\mathfrak{p}$ in $K$ given by $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ we have $f_{\mathfrak{p}|p} = 1$. But this implies that $p$ splits completely in $K$. By construction of $M$, we find that $f_n(x)$ has a zero modulo $\mathfrak{P}$, and then $f_{\mathfrak{P}|p}$ implies that $f_n(x)$ has a zero modulo $p$.

Consequently, this implies $p = x^2 + ny^2$, as $f_n(x)$ satisfies the equivalence, and thus, by Theorem 4.1.3, we find that $p$ splits completely in $L$. But this implies that we have $p \in \mathcal{S}_{L/\mathbb{Q}}$, and thus $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \dot{\subset} \mathcal{S}_{L/\mathbb{Q}}$, since only the set of primes dividing $n$ or the discriminant of $f_n(x)$ were not taken into consideration, which is a finite set. Theorem 3.4.16 tells us that we have $L \subset M$, and therefore we have

$$[L : K] \leq [M : K] \leq \deg(f_n(x)) = [L : K],$$

from which we immediately find that $L = M$. So $f_n(x)$ is indeed the minimal polynomial of some primitive element of the ring class field $L$. □

### 4.2.2 Applications of the Main Theorem

We now discuss a few applications of the Main Theorem. First, we work out a specific example in which $n$ equals 15, to illustrate the theorem. Then, the results from section 1.2 are discussed to show how they can be used to compute the ring class fields of quadratic fields.

**Example 4.2.2.** *(Example for the case $n = 15$) Let $p$ be a prime not dividing 15, then*

$$p = x^2 + 15y^2 \iff p \equiv 1, 4 \bmod 15.$$

*Proof.* First, let us look at the form class group $C(-60)$. It is easy to show that $x^2+15y^2$ and $3x^2+5y^2$ are the only reduced forms in this group, and thus we have $h(-60) = 2$. So the Main Theorem tells us there is an extension $\mathbb{Q}(\sqrt{-15}) = K \subset L$ of degree 2, such that $L = K(\alpha)$ is the ring class field of the order $\mathbb{Z}[\sqrt{-15}]$, where $\alpha$ is a real algebraic integer in $L$.

In Example 3.1.3, we saw that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$, and thus we can compute the conductor of the order is $f = 2$. Now let $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ denote the non-trivial element of this group (complex conjugation), and let $\sigma \in \mathrm{Gal}(L/K)$ denote the non-trivial element of this group. Then we find that $\tau(\alpha) = \alpha$ and $\sigma(\alpha) \neq \alpha$. If we set $\beta = \alpha - \sigma(\alpha)$, then we find $\beta \neq 0$ with $\tau(\beta) = \beta$ and $\sigma(\beta) = -\beta$, from which we obtain $\sigma(\beta^2) = \beta^2$. So $\beta^2$ is an algebraic integer in $\mathbb{Q}$, as it is invariant under both $\sigma$ and $\tau$, and thus we find $\beta^2 \in \mathbb{Z}$. Since $\alpha$ was real, we find that $\beta$ is real and we have $L = K(\beta)$, as $\sigma(\beta) \neq \beta$ and $[L : K] = 2$. So we find that we can write $L = K(\sqrt{m})$, where $m$ is a positive squarefree integer.

Since $L$ is the ring class field of an order of conductor 2, we see that any prime of $K$ that ramifies in $L$ must divide the modulus $2\mathcal{O}_K$. Let $p$ be a prime that divides the number $m$. Suppose that $p$ is odd not dividing 15, then we see that $p$ ramifies in $M = \mathbb{Q}(\sqrt{m})$, as we can write $p\mathcal{O}_M = (p, \sqrt{m})^2$. Now this implies that $p$ ramifies in $L$ as well, and since the only primes ramifying in $K$ are the primes dividing $d_K = -15$, we find that the only primes that can divide $m$ are the primes $2, 3$ and 5. This gives us 7 possible options for $m$: 2, 3, 5, 6, 10, 15 and 30.

The corresponding minimal polynomial $f_n(x)$ is $f_n(x) = x^2 - m$ and if $p$ is an odd prime not dividing 15, it does not divide $m$, and therefore does not divide the discriminant of $f_n(x)$. The equivalence in the Main Theorem implies that such a prime $p$ is of the form $x^2 + 15y^2$ if and only if $\left(\frac{-15}{p}\right) = 1$ and $x^2 \equiv m \bmod p$ has an integer solution, or equivalently $\left(\frac{m}{p}\right) = 1$. If we look at the prime 19, we see that $19 = 2^2 + 15 \cdot 1^2$, so this implies that $\left(\frac{m}{19}\right) = 1$, which, out of the possible $m$ listed, is only true when $m$ equals 5, 6 or 30. The next prime of the given form is $31 = 4^2 + 15 \cdot 1^2$, and this implies $\left(\frac{m}{31}\right) = 1$. This leaves only $m = 5$ as valid choice, so we find that $L = K(\sqrt{5})$, and consequently $p = x^2 + 15y^2$ if and only if $\left(\frac{-15}{p}\right) = 1$ and $\left(\frac{5}{p}\right) = 1$. By applying the quadratic reciprocity law (Theorem 1.1.4), it is straightforward to show that this is equivalent to

$$p = x^2 + 15y^2 \iff p \equiv 1, 4 \bmod 15. \qquad \square$$

Now recall the results from Theorem 1.2.4. For $n = 27$, we see that the polynomial $f_{27}(x) = x^3 - 2$ is a polynomial satisfying the equivalence of Theorem 4.2.1. But this implies that $L = K(\sqrt[3]{2})$ is the ring class field of the order $\mathbb{Z}[\sqrt{-27}]$ in $K = \mathbb{Q}(\sqrt{-3})$. In the same way, we see that $f_{64}(x) = x^4 - 2$ satisfies the equivalence, such that $M = N(\sqrt[4]{2})$ is the ring class field of the order $\mathbb{Z}[8i]$ in $N = \mathbb{Q}(i)$.

Theorem 4.2.1 tells us that determining the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ is equivalent to finding a polynomial $f_n(x)$ satisfying the equivalence. In general, it is still hard to compute the ring class field, as the proof of the Main Theorem gives no explicit construction. There are methods to determine this field, which are described in Chapter III of Cox, see [Cox13].

# Chapter 5

# Related results

The final chapter discusses results related to the Main Theorem, and all other results described in the previous chapters. We first discuss some results by Lenstra, Stevenhagen and Jansen on Mersenne primes of the form $x^2 + dy^2$, and the divisibility properties of $x$ for those representations. Then, we look into the results of Berrizbeitia, Luca and Mendoza on Fibonacci numbers with prime index $p$.

From these results and the methods used in the proofs, we will obtain a similar expression for Lucas numbers with prime index $p$, and formulate some conjectures about these Lucas numbers.

## 5.1 Mersenne primes

In the paper of Lenstra en Stevenhagen (see [LJS00]), the main result is the following theorem.

**Theorem 5.1.1.** *Let $M_l = 2^l - 1$ be a Mersenne prime with $l \equiv 1 \bmod 3$. Then there are $x, y \in \mathbb{Z}$ such that $M_l = x^2 + 7y^2$, and furthermore $x$ is divisible by 8.*

The proof of the theorem relates the Artin symbols of the primes lying over $M_l$ in $\mathbb{Q}(\sqrt{-7})$ to the Artin symbols of the primes lying over $M_l$ in $\mathbb{Q}(\sqrt{2})$.

A generalization of this theorem can be found in the Master's thesis of Jansen (see [Jan02, Thm. 4.2, p. 34]).

**Theorem 5.1.2.** *Let $d = 2^n - 1$ be a squarefree integer with $n$ odd. Let $M_l$ be a Mersenne prime with $l \equiv 1 \bmod n$. If there are $x, y \in \mathbb{Z}$ such that $M_l = x^2 + dy^2$, then $x$ is divisible by 8.*

The proof operates in cyclic extensions of degree 4 over the field $\mathbb{Q}(\sqrt{-2d})$. In the next chapter we attempt to prove similar congruence condition for Lucas primes.

## 5.2 Fibonacci and Lucas numbers

The Fibonacci numbers are the defined by the recursive relation

$$F_{n+2} = F_{n+1} + F_n, \qquad F_0 = 0,\ F_1 = 1.$$

For any Fibonacci number with index $n \geq 5$, it can be shown that $F_n$ can only be prime whenever $p$ is prime. In the paper of Berrizbeitia, Luca and Mendoza, see [BLM15], the following theorem is proven.

**Theorem 5.2.1.** *Let $p$ be a prime number such that $p \equiv 3 \bmod 4$. Then there are integers $x, y$ such that*

$$4F_p = 5x^2 + py^2.$$

The proof of the theorem makes use of Galois theory, the norm function and some properties of the ring of algebraic integers of number fields. Now let us look at the Lucas numbers, which are similar to the Fibonacci numbers, as they satisfy the recursive relation

$$L_{n+2} = L_{n+1} + L_n, \qquad L_0 = 2,\ L_1 = 1.$$

It can be shown that $L_n$ can be prime for $n > 0$ only if $n$ is prime or a power of 2. In the case where $p$ is prime, we prove the following theorem, using the same techniques as in [BLM15].

**Theorem 5.2.2.** *Let $p$ be a prime number such that $p \equiv 3 \bmod 4$. Then there are integers $x, y$ such that*

$$4L_p = x^2 + 5py^2.$$

*Proof.* If we let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = 1 - \alpha = \frac{1-\sqrt{5}}{2}$, then we have

$$L_n = \frac{\alpha^n + \beta^n}{\alpha + \beta}.$$

Let $\zeta_n$ denote a primitive $n$-th root of unity, then this formula leads to the identity

$$L_n = \prod_{t=1}^{n-1} (\alpha + \beta\zeta_n^t).$$

Let $p$ be a prime such that $p \equiv 3 \bmod 4$, set $M = \mathbb{Q}(\sqrt{5}, \zeta_p)$ and set $K = \mathbb{Q}(\sqrt{5}, \sqrt{-p})$. Now, we define $\gamma = \alpha + \zeta_p\beta \in M$ and $\Gamma = N_{M/K}(\gamma) \in K$. By using the facts about the Galois group of $M$ and its subfields, as described in [BLM15], we find that $\mathrm{Gal}(M/\mathbb{Q}) = \langle\tau\rangle \times \langle\sigma_5\rangle$, where $\tau$ denotes a generator of $\mathrm{Gal}(M, \mathbb{Q}(\sqrt{5}))$, and $\sigma_5$ satisfies $\sigma_5(\zeta_p) = \zeta_p$ and $\sigma_5(\sqrt{5}) = \sqrt{5}$.

It follows that $\mathrm{Gal}(M/K)$ is generated by $\tau^2$. If we let $R$ be the set of quadratic residues in $(\mathbb{Z}/p\mathbb{Z})^*$, this fact show that

$$\Gamma = \prod_{r \in R} (\alpha + \zeta_p^r \beta).$$

Since $\tau(\zeta_p) = \zeta_p^g$ for some generator $g$, which neccesarily is not a quadratic residue in $(\mathbb{Z}/p\mathbb{Z})^*$, we find $L_p = \Gamma\tau(\Gamma)$. Now if we consider $\sigma_5(\Gamma)$, we find that

$$\sigma_5(\Gamma) = \prod_{r \in R} (\beta + \zeta_p^r \alpha) = \prod_{r \in R} \zeta_p^r (\alpha + \beta\zeta_p^{-r}) = \prod_{r \in R} (\alpha + \beta_p^{-r}),$$

where the last identity follows from the fact that the sum of the quadratic residues in $(\mathbb{Z}/p\mathbb{Z})^*$ is congruent to 0 modulo $p$.

The congruence $p \equiv 3 \bmod 4$ implies that $-1 \in R$, and consequently we find that $\sigma_5(\Gamma) = \tau(\Gamma)$, or equivalently $\tau\sigma_5(\Gamma) = \Gamma$. This implies that $\Gamma \in \mathbb{Q}(\sqrt{-5p})$, the subfield of $K$ invariant under $\tau\sigma_5$. As $\Gamma$ is an algebraic integer, this implies that $\Gamma = s + t\sqrt{-5p}$ for some rational numbers $s, t$ such that $2s$ and $2t$ are integers. From this we immediately find

$$4L_p = \Gamma\tau(\Gamma) = 4(s + t\sqrt{-5p})(s - t\sqrt{-5p}) = (2s)^2 + 5p(2t)^2,$$

and the result is proven. □

Given the expression for Lucas numbers with prime index from Theorem 5.2.2, we look for divisibility properties, or congruence conditions, on the numbers $x$ and $y$ in these representations. In Table 5.1, one can see the values of $x$ and $y$ for the first few values of $p$, where the second column shows wether or not $L_p$ is prime. Computation of these numbers was done by using MAGMA, see [BCP97]. The code can be found in the Appendix.

| $p$ | $L_p$ | prime | $x$ | $y$ |
|---|---|---|---|---|
| 3 | 4 | no | $1; 4$ | $1; 0$ |
| 7 | 29 | yes | 9 | 1 |
| 11 | 199 | yes | 24 | 2 |
| 19 | 9349 | yes | 154 | 12 |
| 23 | 64079 | no | $209; 251$ | $43; 41$ |
| 31 | 3010349 | yes | 1149 | 263 |
| 43 | 969323029 | no | 35434 | 3492 |
| 47 | 6643838879 | yes | 10996 | 10610 |
| 67 | 100501350283429 | no | 7170074 | 1023012 |
| 71 | 688846502588399 | yes | 23074501 | 2502367 |
| 79 | 32361122672259149 | yes | 138956811 | 16698025 |
| 83 | 221806434537978679 | no | $552136416; 59696424$ | $37460698; 46144406$ |

Table 5.1: Primes $p \equiv 3 \bmod 4$ and the values $x, y$ for the representation(s) $4L_p = x^2 + 5py^2$.

The only two congruences found, are ones that can be proven using the expression $L_p = \alpha^p + \beta^p$ from Theorem 5.2.2. These congruences are described in the next proposition.

**Proposition 5.2.3.** *Let $p \equiv 3 \bmod 4$ be a prime number, and write $L_p = x^2 + 5py^2$, where $x, y \in \mathbb{Z}$ are integers. Then we have $x^2 \equiv 1 \bmod 5$ and $x^2 \equiv 4 \bmod p$.*

*Proof.* We use the identity

$$L_p = \frac{(1+\sqrt{5})^p + (1-\sqrt{5})^p}{2^p}.$$

First, we consider the congruence modulo 5. As $p \equiv 3 \bmod 4$, we see that $2^p \equiv 2^3 \equiv -2 \bmod 5$. If we write $(1+\sqrt{5})^p = \sum_{k=0}^{p} \binom{p}{k} \sqrt{5}^k$, we see all odd terms cancel to the corresponding terms in $(1-\sqrt{5})^p$, and all even terms are divisible by 5, except the first term $\sqrt{5}^0 = 1$. This implies that $(1+\sqrt{5})^p + (1-\sqrt{5})^p \equiv 2 \bmod 5$, so we find $L_p \equiv \frac{2}{-2} \equiv -1 \bmod 5$, and therefore $x^2 = 4L_p - 5py^2 \equiv -L_p \equiv 1 \bmod 5$.

Looking again at the expression $(1+\sqrt{5})^p = \sum_{k=0}^{p} \binom{p}{k} \sqrt{5}^k$, we see that all even terms, except for the first term, are divisible by $p$, and therefore we have $\sqrt{5}^0 = 1$. This implies that $(1+\sqrt{5})^p + (1-\sqrt{5})^p \equiv 2 \bmod p$, and from Fermat's Little Theorem we find $2^p \equiv 2 \bmod p$, so that $L_p \equiv 1 \bmod p$. Consequently, we have $x^2 \equiv 4L_p \equiv 4 \bmod p$. □

Thus, we see that $x$ satisfies certain congruence conditions. If we take a look at the examples, we see that both $x$ congruent to 1 and $-1$ appear in the examples in Table 5.1. Also, both $x$ congruent to 2 and $-2$ appear as well. There also is no number dividing all of the $x$ or all of the $y$. So, we attempt to find a different result.

By taking a closer look to the proof of Theorem 5.2.2, we see that if $L_p$ is prime, it is the product of two principal ideals in $K = \mathbb{Q}(\sqrt{-5p})$. If we consider the Hilbert class field of this extension, we find that the primes lying over $L_p$ are in the kernel of the Artin map (for the modulus $\mathfrak{m} = 1$), so $L_p$ splits completely in this field.

**Conjecture 5.2.4.** *Let $p \equiv 3 \bmod 4$ be a prime number such that $L_p$ is prime. Then $L_p = x^2 + py^2$ for some integers $x, y \in \mathbb{Z}$.*

Let $K = \mathbb{Q}(\sqrt{-5p})$ and let $L$ denote the Hilbert class field of $K$. Consider the extension of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-p}) = N$, in which the only prime that ramifies is the prime $p$. Now a prime $p \equiv 3 \bmod 4$ does not ramify in the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})$, so we find that the extension $K \subset K(\sqrt{-p})$ is unramified. This implies that $\sqrt{-p} \in L$. This result can also be derived from the fact that $\sqrt{-p}$ is contained in the *genus field* of $K$, the largest subfield of the Hilbert class field, that is abelian over $\mathbb{Q}$. For more details, see [Cox13, Thm. 6.1, p. 109].

As seen in the proof of the Main Theorem, we can choose $\alpha$ to be a real such that $L = K(\alpha)$. Now the Galois group $\mathrm{Gal}(L \cap \mathbb{R}/\mathbb{Q})$ is isomorphic to $\mathrm{Gal}(L/K)$, which is abelian, as both groups are of the same order, and any element of $\mathrm{Gal}(L/K)$ has a corresponding restriction in $\mathrm{Gal}(L \cap \mathbb{R}/\mathbb{Q})$. But then $L = (L \cap \mathbb{R})(\sqrt{-p}) = L$ implies that $\mathrm{Gal}(N/K)$ is also isomorphic to $\mathrm{Gal}(L \cap \mathbb{R}/\mathbb{Q})$, and therefore is abelian.

To find a representation of the prime $L_p$ by the form $x^2 + py^2$, a possible is to find a relation between the Hilbert class field $L$ and the ring class field of $\mathbb{Z}[\sqrt{-p}]$. However, we have that 5 ramifies in $L$, so that the primes in $\mathbb{Q}(\sqrt{-p})$ dividing 5 ramify in $L$ as well. To relate these fields, we thus need to consider extensions with conductor divisible by 10.

**Conjecture 5.2.5.** *Let $p \equiv 3 \bmod 4$ be a prime number. Then $L_p = x^2 + py^2$ for some integers $x, y \in \mathbb{Z}$.*

A method of proving this conjecture might be by the norm function, in a way similar to how it was used in Theorem 5.2.2. For Fibonacci numbers $F_p$, where $p \equiv 1 \bmod 4$ is prime, this result was proven in [AGBL15] using norms.

# Appendix

## Code for computing $x$ and $y$ in the representation $4L_p = x^2 + 5py^2$

The code below was used to compute the values in Table 5.1. Originally, the commands used were functions for solving these equations, using the built-in functions in MAGMA, listed below.

```
p:=3;
Lp:=Lucas(p);
f:=5*x^2+p;
T:=Thue(f);
Solutions(T,4*Lp);
```

Due to limitations on computation time on the online calculator, the code was altered to compute $x$ and $y$ for more values of $p$. The final code is listed below.

```
p:=3;
Lp:=Lucas(p);
a:=0;
b:=0;
i:=0;
for i in [1 .. Floor(Sqrt(4*Lp/(5*p)))] do
        y:=4*Lp-5*p*i^2;
        if IsIntegral(Sqrt(y)) then a:=y;
                b:=5*p*i^2;
                [Sqrt(a),Sqrt(b/(5*p))];
        end if;
end for;
Lp;
IsPrime(Lp);
```

# References


[AGBL15] Juan José Alba González, Pedro Berrizbeitia, and Florian Luca. On the formula $F_p = u^2 + pv^2$. *International Journal of Number Theory*, 11(01):185–191, 2015.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BLM15] Pedro Berrizbeitia, Florian Luca, and Alberto Mendoza. Quadratic forms representing the $p$-th Fibonacci number. 2015, arXiv:1502.04346v1 [math.NT].

[Cox13] David A. Cox. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc., second edition, 2013.

[IR82] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer New York, 1982.

[Jan96] Gerald J. Janusz. *Algebraic Number Fields*. American Mathematical Soc., second edition, 1996.

[Jan02] Bas Jansen. Mersenne primes of the form $x^2 + d \cdot y^2$. Master's thesis, Universiteit Leiden, the Netherlands, 2002.

[LJS00] H.W. Lenstra Jr and P. Stevenhagen. Artin reciprocity and Mersenne primes. *Nieuw Arch. Wisk.*, 5(1), 2000.

[Mar77] Daniel A. Marcus. *Number Fields*. Springer-Verlag New York Inc., 1977.

[Neu86] Jürgen Neukirch. *Class Field Theory*. Springer-Verlag Berlin Heidelberg, first edition, 1986.

[Ste10] Peter Stevenhagen. Algebra 2. Course Notes, Universiteit Leiden, 2010. `http://websites.math.leidenuniv.nl/algebra/algebra2.pdf`.