Primes of the form x^2-ny^2

Gool, J. van

Universiteit Leiden
Mathematisch Instituut

Master Thesis

Primes of the form $x^2 - ny^2$

Author:
Joris van Gool

Supervisor:
Prof.dr. P. Stevenhagen

April 4, 2020

Contents

1 Introduction

In 1640 Fermat mentions the problem of what primes can be written as the sum of two squares, $p = x^2 + y^2$, in a letter. This marks the start of a long series of discoveries. After Fermat, a century later, in 1744, Euler writes *Theoremata circa divisores numerorum in hac forma paa±qbb contentorum* [1, Series 1, Vol. 2, p. 194-222] about the possible prime divisors of solutions of $nx^2 \pm my^2$ for given m, n. He already examines a wider range of problems and finds solutions for quite a few m, n. His solutions are not proofs however, and can best be described as observations that have now been proved to be correct. More generalization and better understanding came when Lagrange introduced discriminants, equivalent forms and reduced forms [2]. Continuing the exploration of forms, Gauss introduced the concept of proper equivalence and shows that equivalence classes of reduced forms have a natural group structure [3].

All of this is being shown without class field theory, which later proves to be a central element in solving these kinds of problems. To introduce class field theory we first have to look at the ring whose field of fractions we will be using:

$$\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$$

In this quadratic order we can factor $x^2 + ny^2$ like this

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

with $(x+y\sqrt{-n}), (x-y\sqrt{-n}) \in \mathbb{Z}[\sqrt{-n}]$. These rings are not necessarily unique factorisation domains, which poses a problem. Some p might "factor" but not into elements in the ring. This is where Kummer comes in, he introduced ideals. The first time he mentions them is in a paper in 1847 [4], referring to them as *Ideale Zahlen*. He invents them while trying to prove Fermat's last theorem when he discovers that some number rings don't have unique factorisation. The reparation, provided by Dedekind[5], consists in using the integral closure of a number ring, which is a *Dedekind domain*. In these rings, we have *unique prime ideal factorization*: every non-zero ideal factors uniquely into a product of prime ideals. Now we can say that if $p = x^2 + ny^2$ there are primes $\mathfrak{p}$ and $\mathfrak{p}'$ such that

$$\mathfrak{p}\mathfrak{p}' = (p) \tag{1}$$

with $\mathfrak{p} = (x - y\sqrt{-n})$ and $\mathfrak{p}' = (x + y\sqrt{-n})$. So all primes p of the form $x^2 + ny^2$ factor into two ideals in $\mathbb{Z}[\sqrt{-n}]$. The converse is not true. In the factorisation we see that the

ideals are generated by $(x \pm y\sqrt{-n})$ which makes them principal. One might wonder what happens when an ideal $\mathfrak{p}$ in (1) is non-principal. Later in section 4 we will show that such p are represented by a binary quadratic form (see section 2) with the same discriminant, $-4n$, but not $x^2 + ny^2$. In order to check whether a prime $p \nmid 4n$ is the product of two ideals as in (1) we can simply check whether $-4n$ is a square modulo that prime. If it is, then it does factor into two ideals. Finally we can say something about the density of primes represented by a given form. A range of thoughts on this subject for binary quadratic forms of negative discriminant can be found in "Primes of the form $x^2 + ny^2$" by David A. Cox [6].

In this text we will focus on $x^2 - ny^2$ with n positive which makes the discriminant of these forms, $4n$, positive. We will shortly discuss the case of n being a square later in the introduction but this will not require any of the more complicated mathematics used for the rest of the text. Therefore we will assume n is not a square unless indicated otherwise. We will first go over Cox's case of the form $x^2 + ny^2$ of negative discriminant $-4n$. These forms are positive definite which by definition means they only have positive outcomes for $x, y \in \mathbb{Z}$. While doing so we will look at the differences with the indefinite case, named that way because the form is able to take both positive and negative values. The first clear difference is that in the case of $x^2 + ny^2 = p$ the prime p can only be positive. For $x^2 - ny^2$ it can be equal to p or to $-p$ and one does not necessarily imply the other. An extra condition to ensure there is a solution with p positive will be that the norm of the element α generating the principal ideal $\mathfrak{p} = \alpha\mathcal{O}$ has to be $p = N(\alpha)$ with p positive. Although we will only explore the way to find positive p, we will discuss what would have to be done differently to obtain a solution for positive and negative p.

We have made a statement about the meaning of p being represented by the form $x^2 + ny^2$ in terms of ideals of $\mathbb{Z}[\sqrt{-n}]$. This raises the question, how can it be known whether p can be written as the product of two principal ideals as in (1). Class field theory, not known to Gauss and his predecessors, gives us a field in which exactly every principal prime ideal that split in $\mathbb{Z}[\sqrt{n}]$ splits completely: the ring class field. The result obtained using this ring class field is very similar to the result found in "Primes of the Form $x^2 + ny^2$" by David A. Cox [6, Thm. 9.2, p. 163]. However, due to the sign change, we will see that differences arise. We will also find that the proof for a specific n in $x^2 - ny^2$ is more complicated than $x^2 + ny^2$ is in the book. The theorem for indefinite forms which resembles theorem 9.2 for positive definite forms in Cox reads:

Theorem 1.1. *For $n \in \mathbb{Z}_{>0}$ not a square and $p \nmid 2n$ prime we have that the equation*

$p = x^2 - ny^2$ has a solution in integers if and only if p splits completely in the narrow ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{n}]$.

To illustrate what this means we will elaborate a little bit. We will use the *narrow* ring class field to get solutions for $p = x^2 - ny^2$ with p *positive*. The first of two inclusions we can use to gain some insight in the theorem starts with the field $\mathbb{Q}(\sqrt{n})$, which contains a maximal order $\mathcal{O}_K$ of infinite index and the order $\mathcal{O}$ with index f in $\mathcal{O}_K$:

$$K = \mathbb{Q}(\sqrt{n}) \qquad \supset \qquad \mathcal{O}_K \qquad \overset{f}{\supset} \qquad \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$$

Here $\mathcal{O}_K$ is the Dedekind domain having unique prime ideal factorization and $\mathcal{O} \subset \mathcal{O}_K$ is an order having "singular primes" dividing f. The conductor f is the index of $\mathcal{O}$ in $\mathcal{O}_K$ and is related to the discriminant of the form $x^2 - ny^2$ as will be explained below, the discriminant being $\Delta = 4n$. Using the discriminant we can make certain observations concerning the conductor. As we know from algebraic number theory if $n \not\equiv 1 \mod 4$ is squarefree, the order $\mathbb{Z}[\sqrt{n}]$ is maximal. We find that if $n \not\equiv 1 \mod 4$ then the discriminant can be written as $\Delta = f^2 \cdot 4m$ with m squarefree and f the conductor. The other case where $n \equiv 1 \mod 4$ we get that $\Delta = f^2 m$ with m squarefree and f the conductor. When $n \equiv 1 \mod 4$ the prime 2 is unramified in the order $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ of discriminant n.
The second set of inclusions leads up to the narrow ring class field, H_f^+. This is the narrow ring class field of $\mathcal{O}$. As we will soon find out and later prove its properties provide the solution to our main problem. We denote the Hilbert class field H and the narrow Hilbert class field H^+:

$$\mathbb{Q} \qquad \subset \qquad K = \mathbb{Q}(\sqrt{n}) \qquad \subset \qquad H^+ \qquad \subset \qquad H_f^+$$

The first field of interest is $K = \mathbb{Q}(\sqrt{n})$, the quadratic number field that contains the zeroes of $x^2 - n$. This is the smallest field in which we can factor the function $x^2 - ny^2$ into $(x - y\sqrt{n})(x + y\sqrt{n})$. The field K is contained in the narrow Hilbert class field of K which we could also call the narrow ring class field of the ring of integers. The final field is the narrow ring class field, H_f^+, of the quadratic order $\mathcal{O}$. The desirable property of the ring class field is that if and only if a prime $\mathcal{O} \ni \mathfrak{p} \nmid f$ splits completely in the ring class field, then it was principal in the corresponding order:

$$\mathfrak{p} \nmid f \text{ splits completely in } H_f^+ \iff \mathfrak{p} = (\pi) \text{ with } \pi \in \mathcal{O} \text{ and } N(\pi) > 0$$

As will be discussed later, dropping the "narrow" removes the requirement for positive norm.

$$\mathfrak{p} \nmid f \text{ splits completely in } H_f \iff \mathfrak{p} = (\pi) \text{ with } \pi \in \mathcal{O}$$

This is of course a fairly strange relation which raises the question how we can find such a specific field. In section 4 of this thesis we will describe an isomorphism between the (narrow) class group of an order and the Galois group of its (narrow) ring class field.

$$\mathrm{Cl}^+(\mathbb{Z}[\sqrt{n}]) \cong \mathrm{Gal}(H_f^+/K)$$

It should also be noted that each f corresponds to a unique order in $\mathcal{O}_K$. The class structure of the class field in this order is not necessarily unique and the ring class field can also be the same for several orders. Each order does of course only admit one class group and one ring class field.

Finally we will discuss $n = m^2$ being a square and introduce the density of primes in a solution. For $x^2 + m^2y^2$ we can use the approach described in Cox and it will still work. For $x^2 - m^2y^2$ we can factor the equation into $(x - my)(x + my)$ without needing any elements not present in $\mathbb{Z}$. We assume without loss of generality that $x, y > 0$. This means that $x^2 - m^2y^2$ is not a prime unless either $x - my$ or $x + my$ is 1. Since $x + my$ cannot be 1 unless $x - my$ is also 1 this yields no solutions. For $x - my = 1$ we have that $x = 1 + my$ so $x + my = 2my + 1$. This shows that for $n = m^2$ a square, the prime p is represented if and only if $p = 2my + 1$ for some y. This is a splitting condition, p needs to split completely in $\mathbb{Q}(\zeta_{2m})$. As a congruence condition this would be $p \equiv 1 \mod 2m$.

What fraction of primes is represented by $x^2 - m^2y^2$ and thus equal to $1 \mod 2m$ can be calculated using Dirichlet's theorem on arithmatic progressions[7][8]. Later this Theorem will return as a special case of the Chebotarev Density Theorem.

Theorem 1.2. *For $k, l \in \mathbb{Z}$ relative prime there are infinitely many primes p with $p \equiv k \mod l$. And for x going to infinity a fraction $\frac{1}{\varphi(l)}$ of primes are $p \equiv k \mod l$.*

This theorem tells us that the collection of all primes coprime to l is equidistributed in $(\mathbb{Z}/l\mathbb{Z})^*$.

Corollary 1.3. *$x^2 - m^2y^2$ represents a fraction $\frac{1}{\varphi(2m)}$ of all primes.*

This comes from combining the theorem with the result that $x^2 - m^2y^2 = p$ only for $p \equiv 1 \mod 2m$.

2 Form class group

We define a binary quadratic form to be any $f(x,y) = ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ with $a,b,c \in \mathbb{Z}$. This binary quadratic form has discriminant $\Delta = b^2-4ac$ and thus $x^2 \pm ny^2$ has discriminant $\Delta = 0^2 - 4\cdot 1 \cdot \pm n = \mp 4n$. If there are $d,e \in \mathbb{Z}$ such that $f(d,e) = m$ with m some integer we say that $f(x,y)$ represents m. In essence one could also state that we are looking for which values of p are represented by a certain f. In order to make statements about forms it is desirable to have a solid understanding of the set of all forms. In order to reduce the number of forms that we need to look at we first define primitive forms to be forms such that a,b,c are relatively prime and therefore the form isn't a multiple of another form. Non-primitive forms are of little interest as the only prime they can represent is $gcd(a,b,c)$ if it is prime. This already reduces the number of forms significantly but the number is still infinite. We will refer to the collection of all primitive forms as $\mathcal{F} = \{\ (a,b,c) \mid a,b,c \in \mathbb{Z}, \gcd(a,b,c) = 1\}$. A triple (a,b,c) corresponds to the form $ax^2+bxy+cy^2$.

Some forms in $\mathcal{F}$ are essentially the same and differ only by a linear transformation. In order to make this clear we first look at binary quadratic forms as a function from $\mathbb{Z}^2$ to $\mathbb{Z}$:

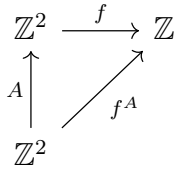
$$f : \mathbb{Z}^2 \to \mathbb{Z}$$

$$(x,y) \to f(x,y)$$

Now we can apply a linear transformations to $\mathbb{Z}^2$ which retains all the values that are in the codomain of f. This is a linear function $A : \mathbb{Z}^2 \to \mathbb{Z}^2$ that we apply before f. This gets us a function $f^A = f(A(x,y))$. Since A is a linear transformation we can take it to be an integer 2×2 matrix. The discriminant of f^A only differs from the discriminant of f by a factor equal to the square of the determinant of A.

$$\operatorname{disc}(f^A) = (\det(A))^2 \cdot \operatorname{disc}(f) \tag{2}$$

The following commutative diagram illustrates the relations between A, f and f^A:



As we want to reduce the number of forms we would like to use A to obtain an equivalence relation. Using the function A we have transitive and reflexive properties but just taking

any integer matrix A will not do for the symmetry property of an equivalence relation. We need the matrix A to be invertible for the symmetric property to hold, integer matrices are only invertible if they have determinant ± 1. This also nicely lines up with (2) as that also means the discriminant stays the same. The group of integer matrices with determinant ± 1 is called $\mathrm{GL}_2(\mathbb{Z})$. Because the discriminant never changes we can look at $\mathcal{F}_\Delta$, all forms of discriminant Δ, instead of the entire collection $\mathcal{F}$. Now we can quotient out by the group action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathcal{F}_\Delta$. This turns it into an orbit space $\mathcal{F}_\Delta/\mathrm{GL}_2(\mathbb{Z})$ where every orbit is a set of forms that represents the same numbers. Logically we call forms that are in the same orbit *equivalent forms*. Instead of $\mathrm{GL}_2(\mathbb{Z})$ we will use $\mathrm{GL}_2(\mathbb{Z})/(\pm\mathrm{Id})$ because the identity and minus the identity do the same thing when applied to forms. Gauss discovered that if you use $\mathrm{SL}_2(\mathbb{Z})/(\pm\mathrm{Id})$ instead of $\mathrm{GL}_2(\mathbb{Z})/(\pm\mathrm{Id})$ on a collection of forms of the same discriminant the resulting collection admits to a natural group structure[3, section V]. The composition used by Gauss is relatively difficult as these sets of forms don't obviously form a group and was later revisited by Dirichlet [9, supplement X] and others for simplification. The main problem with composition is that the forms are in equivalence classes and the outcome of composition depends on the representative chosen. We need to use $\mathrm{SL}_2(\mathbb{Z})/(\pm\mathrm{Id})$ instead of $\mathrm{GL}_2(\mathbb{Z})/(\pm\mathrm{Id})$ because we will later find out that the latter identifies all elements of $\mathcal{F}_\Delta$ with their inverse. This destroys the natural group structure for any group that isn't of order two. The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Which makes the full group

$$\mathrm{SL}_2(\mathbb{Z})/(\pm\mathrm{Id}) = \mathrm{PSL}_2(\mathbb{Z}) = \langle S, T \rangle / (\pm\mathrm{Id})$$

Using the group action of this group on $\mathcal{F}_\Delta$ we get an equivalence relation on all binary quadratic forms of discriminant Δ. We call forms that are equivalent by this relation *properly equivalent*. We obtain a finite number of orbits as will be demonstrated later in this section. Given this equivalence relation we still don't know which forms represent the same value without trying all possible matrices. We need some representative for each of the orbits.
This is where the in section 1 aforementioned reduced forms by Lagrange come in to play. The concept is based on using matrices in $\mathrm{PSL}_2(\mathbb{Z})$ to turn a form into a unique form satisfying certain properties. If two forms can be reduced to a form with those properties and if the result is identical we know that the forms are equivalent by a combination of the matrix used to reduce the first form and the inverse of the matrix used to reduce the second form. The definition of *reduced* for forms $ax^2 + bxy + cy^2$ of negative discriminant is:

$$|b| \leq a \leq c \text{ and if } |b| = a \text{ or } a = c \text{ then } b \geq 0 \tag{3}$$

An easy way to visualise if a form is reduced is to look at the embedding of one of the roots of the form in the upper half of the complex plane. The roots of the form are $\frac{-b\pm\sqrt{\Delta}}{2a}$ with $\frac{-b+\sqrt{\Delta}}{2a}$ in the upper half plane. Because $|b| \leq a$ we see that the real component is between $-\frac{1}{2}$ and $\frac{1}{2}$. The root is outside the unit circle because the absolute value is $\sqrt{\tau\bar{\tau}}$ with $\bar{\cdot}$ complex conjugation and $\tau\bar{\tau} = \frac{c}{a}$ as $f(x,y) = a(x+\tau)(x-\tau)$ and $c \geq a$, as can be seen in figure 1.

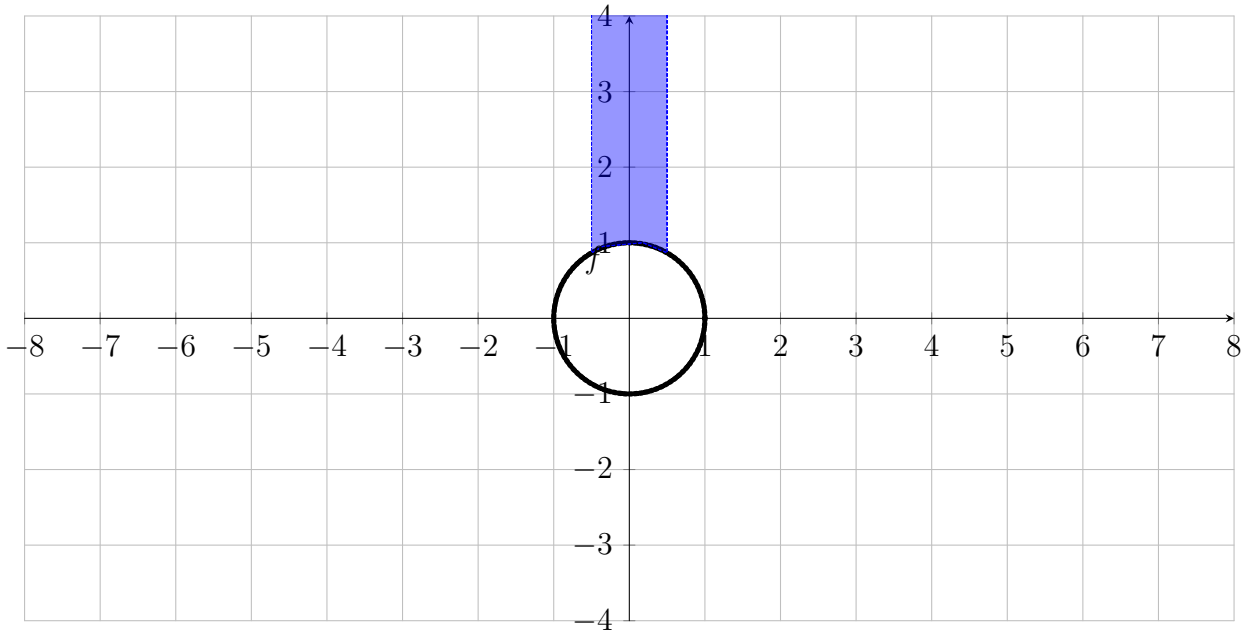


Figure 1: Embedding of the roots of reduced polynomials in $\mathbb{C}$

To show the reduction process in a more intuitive fashion we can investigate the embeddings of the roots in $\mathbb{C}$. This comes down to

$$T(\tau) = \tau + 1$$
$$S(\tau) = \frac{-1}{\tau}$$

As T only changes the b and c of the form, it applies to the real part of the root $\frac{-b+\sqrt{\Delta}}{2a}$ and changes it to $\frac{-b+2a+\sqrt{\Delta}}{2a}$, effectively shifting the root over by 1 on the real axis. The second matrix S turns τ into $-\frac{1}{\tau}$. Graphically, in Figure 1, this would translate to moving it out of or into the unit circle and mirroring the angle in the imaginary axis. Mirroring the angle

in the imaginary axis does not matter for getting the point closer to the reduced area as the reduced area is the same on both sides of the imaginary axis. We reduce the form by applying the following 2 steps starting with the root τ or $\bar{\tau}$ depending on which one is in the upper half plane. Step 1, we apply matrix T until the real part of the root is between $-\frac{1}{2}$ and $\frac{1}{2}$. Then if it is in the blue area it is reduced, if it is not we go to step 2 and apply S shifting the root out of the circle increasing the imaginary part. Now we repeat these steps until our root arrives in the blue area. This always takes a finite number of steps[6, Lemma 11.4, p. 202].
We can prove a nice bound on the number of possible a, b for which a, b, c is reduced by starting with $\Delta = b^2 - 4ac$ and applying that both $|b|$ and a are positive and smaller than c. We get $\Delta \leq c^2 - 4c^2 = -3c^2$ which proves the bound $|b| \leq a \leq c \leq \sqrt{\frac{-\Delta}{3}}$. This combined with the fact that every form is properly equivalent to a reduced form shows that $\#\mathcal{F}_\Delta/\mathrm{PSL}_2(\mathbb{Z}) < \infty$.

As demonstrated we can find a single reduced form for each orbit of properly equivalent forms of negative discriminant. If the discriminant is positive however, we are unable to do so. We can find reduced forms but it turns out that there is finitely many of them all properly equivalent to each other. For positive discriminant we will again have a similar two step algorithm. At the end of this algorithm when a reduced form is found the two steps can be applied again to get another reduced form. All reduced forms properly equivalent to one form are in a cycle and applying the two steps of the reduction algorithm brings you to the next form in the cycle.

We have an analogue of (3) for forms of positive discriminant. A form $f(x, y)$ of positive discriminant is reduced if and only if:

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

In this definition a can also be replaced with c to get an equivalent definition. This definition is again easier to understand looking at the roots $\tau = \frac{-b+\sqrt{\Delta}}{2a}, \sigma(\tau) = \frac{-b-\sqrt{\Delta}}{2a}$ of $f(x, y)$. In this case, a reduced form implies that $0 < \tau < 1$ and $\sigma(\tau) < -1$ or $-1 < \tau < 1$ and $\sigma(\tau) > 1$. Figure 2 illustrates the definition of reduced in terms of the roots of $f(x, y)$ embedded in $\mathbb{R}^2$ as $(\tau, \sigma(\tau))$ in a similar fashion to figure 1.

The highlighted area indicates where a root of the form needs to be located for the form to be considered reduced. The hyperbola is the unit hyperbola $xy = \pm 1$. Applying matrix T to a form shifts the roots of that form by the vector $u = (1, 1)$ as seen in figure 2. Similar

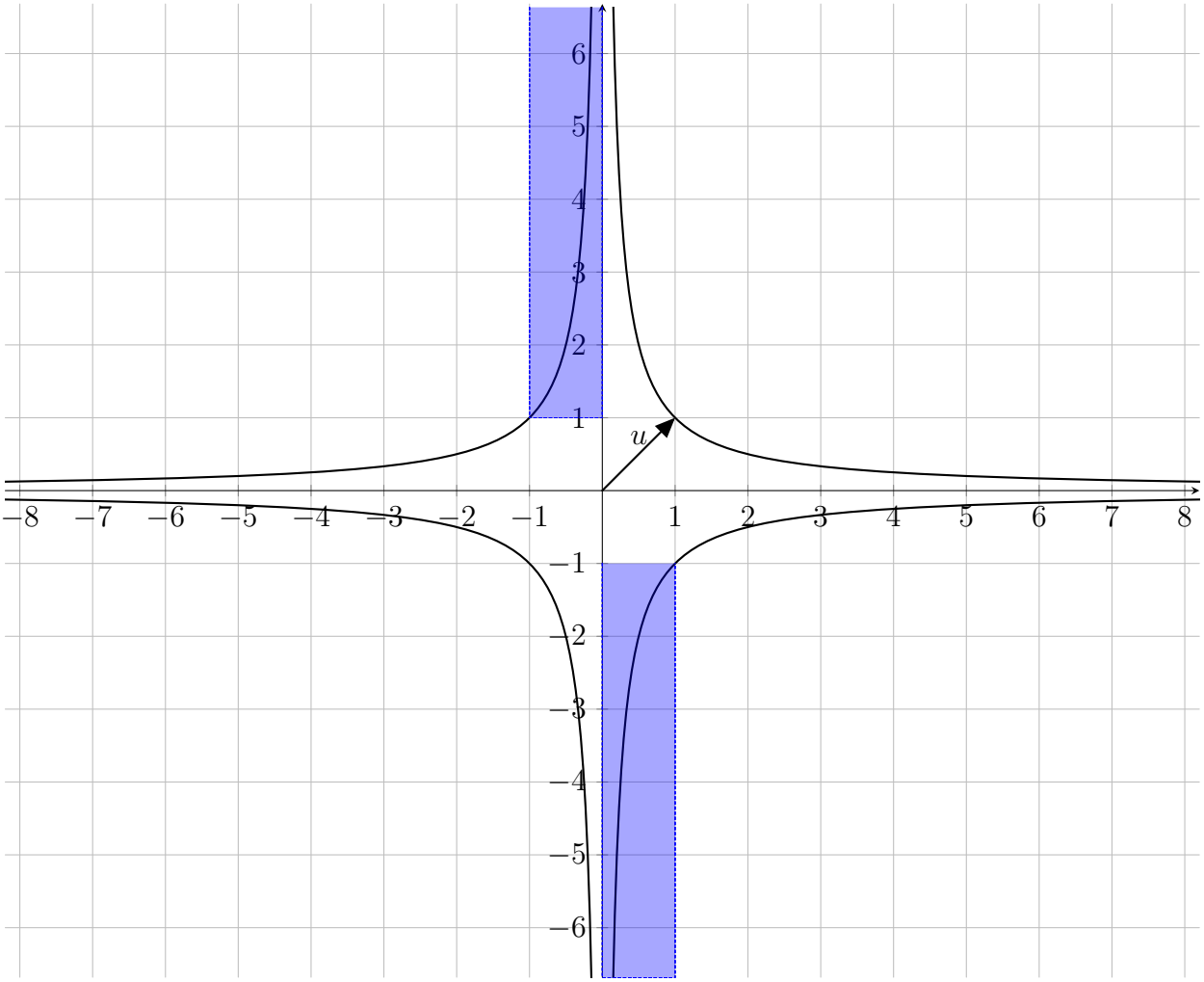


Figure 2: Embedding of the roots of reduced polynomials in $\mathbb{R}^2$. Note vector $u = (1, 1)$.

to the complex case the roots become $\frac{-b+2a\pm\sqrt{\Delta}}{2a}$. This makes both roots shift by one. In the embedding this corresponds to $(x + 1, y + 1)$. Next, we consider the transformation induced in real forms by matrix S, which, analogous to the imaginary forms, changes root τ to $-\frac{1}{\tau}$. The real embedding is somewhat more complicated for these forms. In figure 3 there is an illustration of what happens to the embedding of the roots of a form D when matrix S is applied to it, they get send to L. Both the x and y coordinates are inverted and multiplied by -1. In the figure this moves the x coordinate of the point over the x-axis until it passes the y-axis and subsequently hits the unit hyperbola and similarly the y coordinate over the y-axis until it passes the x-axis and subsequently hits the unit hyperbola. Finally the point is mirrored in the line $y = -x$. This shows us that just like in the imaginary case the reduced area was a choice and instead of $0 < \tau < 1$ we could have chosen $1 < \tau < 2$. The reason for

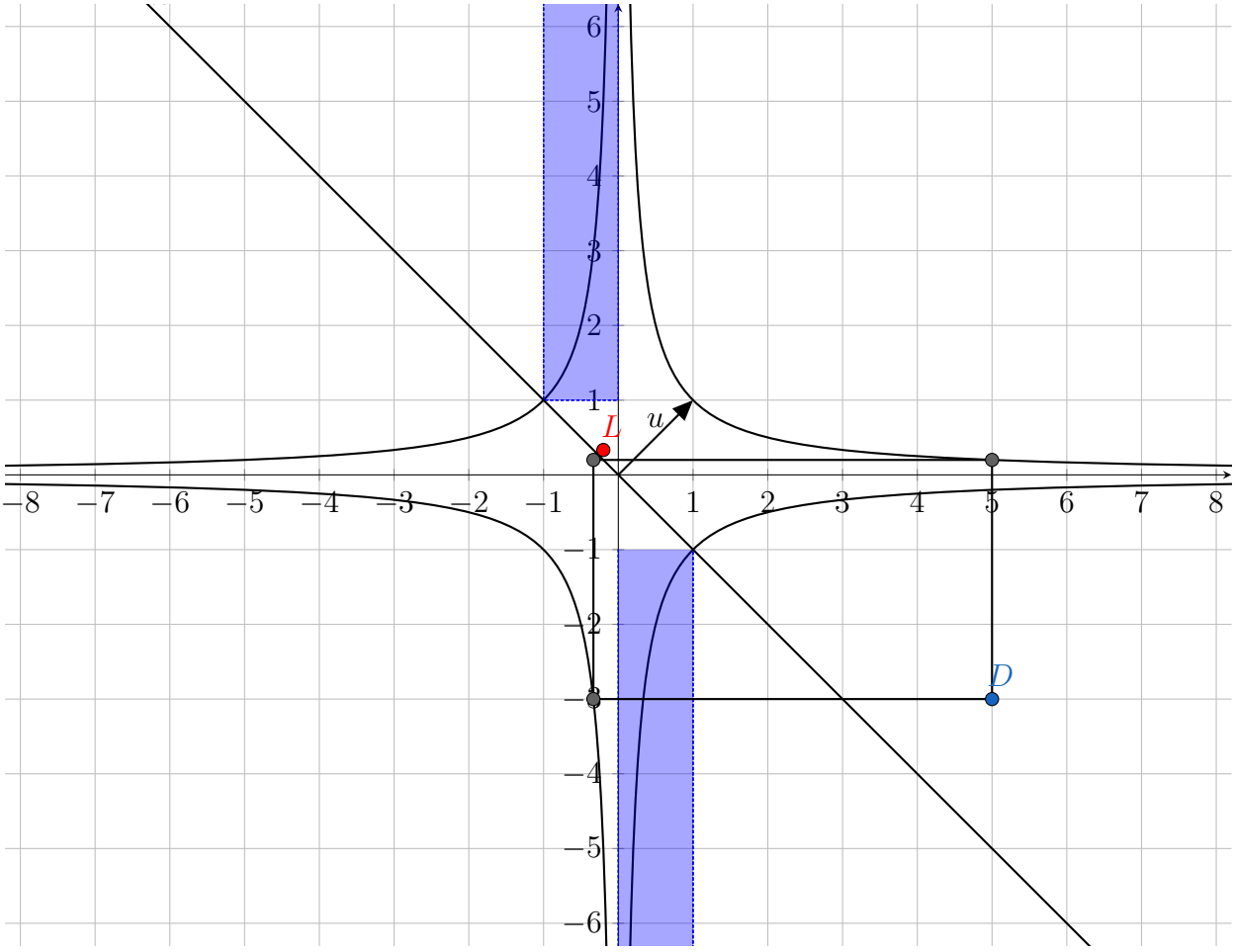


Figure 3: Applying matrix S the form with root D transforming it into a form with root L.

defining reduced as $0 < \tau < 1$ and $\sigma(\tau) < -1$ will become apparent when we start looking at class groups.

Similar to the negative discriminant we also want to be able to reduce forms of positive discriminant to their cycle. The algorithm to do this is explained in detail in quite a few computational number theory texts[10, p.263][11]. The real algorithm works similarly to the complex algorithm. This time we apply T to fix b to an interval, then we check if our form is reduced. If it is not S is applied to the form and we repeat these two steps. A better version of this reduction algorithm is available[10, Def 5.6.4, p. 263]
In order to quickly find the form class group for a specific discriminant it is easy to list all the reduced forms of that discriminant and then order them in cycles. A computer can do this relatively quickly.

3 Narrow class group

As mentioned in the introduction we want to find primes that split into principal ideals $\alpha\mathcal{O}$ for which $N(\alpha) > 0$ in $\mathbb{Z}[\sqrt{n}]$. This is because primes that split into principal ideals satisfy the equation $p = x^2 - ny^2$. Primes that don't split into principal ideals also satisfy some equation of the same discriminant but not this one. The collection of invertible prime ideals modulo the principal invertible prime ideals is called the class group $Cl(K) = I_K/P_K$. The only class in the class group consisting of principal ideals is the identity by definition. The identity class does contain ideals generated by elements of both positive and negative norm. Since we only want ideals with positive norm as these have solutions for $p = x^2 - ny^2$ and not $\pm p = x^2 - ny^2$ we use the narrow class group. The narrow class group is $\mathrm{Cl}^+(K) = I_K/P_K^+$ with P_K^+ the subgroup of all principal invertible ideals represented by an element of positive norm. Even though it is called narrow it is the same size or bigger than the normal class group since $P_K^+ \subset P_K$. Because any ideal generated by a single element of positive norm is a principal ideal. We will see that the case where $P_K^+ = P_K$ does occur later in this section. It is of course very interesting that all primes $p = x^2 - ny^2$ are in the same class in the narrow class group. One might wonder if there is some sort of relation between forms and ideal classes in the narrow class group. As it turns out this relation does exist and works the same for other forms with the same discriminant. Primes represented by those forms aren't principal but they are all in the same class in the narrow class group. In order to find out what primes are represented by a certain form we can use a bijection between the narrow class group $\mathrm{Cl}^+(\mathcal{O})$ and the orbit space $C(\Delta) = \mathcal{F}_\Delta/\mathrm{PSL}_2(\mathbb{Z})$. Thus, $C(\Delta)$ is naturally equipped with a group structure. This is the fundamental discovery of Gauss:

Theorem 3.1. *There is a bijection between the narrow class group $Cl^+(\mathcal{O})$ and $C(\Delta) = \mathcal{F}_\Delta/PSL_2(\mathbb{Z})$ defined by:*

$$\psi : C(\Delta) \to Cl^+(\mathcal{O})$$

$$f(x,y) = ax^2 + bxy + cy^2 \to \mathfrak{a} = \begin{cases} [a, \frac{(-b+\sqrt{\Delta})}{2}] & a > 0 \\ \sqrt{\Delta}[a, \frac{-b+\sqrt{\Delta}}{2}] & a < 0 \end{cases}$$

Proof. An outline for this proof is given in the literature[10, page 229, Theorem 5.2.9][6, page 128]. □

This brings us one step closer to answering the question which primes are represented by certain forms. Figuring out what primes are in a certain class is not the nicest thing to do and we would really like to have a congruence condition. We will explore finding such a

congruence condition in the next section. For now we will discuss implications of theorem 3.1.

So far we have seen quite some differences between the cases $\Delta > 0$ and $\Delta < 0$. For $\Delta > 0$ we might have $-p$ as a solution to our equation and instead of a single reduced form we end up with a cycle of reduced forms. In order to explain both these phenomena we need to have a look at a fundamental difference between $\mathbb{Z}[\sqrt{n}]$ and $\mathbb{Z}[\sqrt{-n}]$ for $n > 0$. As you can see in figure 1 all units are on a circle and for $n \neq 1$ the only units in $\mathbb{Z}[\sqrt{-n}]$ are 1 and -1.

As we can see in figure 2 the units in $\mathbb{R}^2$ are on a hyperbola. The Dirichlet unit theorem shows that the unit group of the maximal order and any suborder is infinite of rank one:

$$\begin{array}{ll} \mathcal{O}_K^* & =< -1 > \times < \epsilon_\Delta > \\ \cup & \\ \mathcal{O}^* & =< -1 > \times < \epsilon_\Delta^k > \end{array}$$

Here ϵ_Δ is the fundamental unit in $\mathcal{O}_K$ of infinite order. This unit is not necessarily in $\mathcal{O}^*$ as $\mathcal{O}^*$ has index $f \neq 1$ in $\mathcal{O}_K^*$. Some power of ϵ_Δ will be in $\mathcal{O}^*$ though, because ϵ_Δ has finite order in the finite multiplicative group $(\mathcal{O}/f\mathcal{O}_K)^*/(\mathbb{Z}/f\mathbb{Z})^*$ and once it is the identity it is in $\mathcal{O}$. In the complex case there is only 1 and -1 as units and by picking our form always in the upper half plane we don't have this problem.

Like mentioned before, in the real case a form can represent $-p$ but not p. If this is the case the narrow class group contains a class of negatively generated principal ideals. If we were to be interested in what form represents $-p$ we could use an involution created by adding the ideal class that contains a prime lying over p with the ideal class containing the negatively generated principal ideals. The resulting ideal class is what forms representing $-p$ map to, this will be illustrated in example 6.1. Sometimes both $-p$ and p are represented by the same form in the real case. For principal ideals this means that the ideal has both a positive and negative generator. The only way for an ideal to have both a positive and negative generator is if the fundamental unit has norm -1. Then you can multiply the generator with positive norm with the fundamental unit to get a generator with negative norm. The existence of a unit of norm -1 implies that $\mathrm{Cl}^+(\Delta) = \mathrm{Cl}(\Delta)$. The cases described above can not both happen at the same time, so either the ideals with generator of norm p and $-p$ are in the same class for all p or they are in different classes for all p.
If the fundamental unit of $\mathcal{O}_K$ has norm -1 but the fundamental unit of $\mathcal{O}$ does not, which happens when k is even, then in the narrow class group of $\mathcal{O}$ the primes generated by positive and negative elements are not in the same class.

The following exact sequence illustrates the difference between the narrow and regular class group quite well:

$$0 \to [\sqrt{\Delta}] \to \mathrm{Cl}^+ \to \mathrm{Cl} \to 0$$

Which shows that the narrow class group is either twice as big or equal to the regular class group depending on whether $[\sqrt{\Delta}]$ is part of P_K^+.

4 Ring class fields

In Theorem 1.1 we wanted primes to split completely in some field H_f. This field is the ring class field, an abelian extension of K. In this field all primes in K that ramify in H_f divide $\mathfrak{f} = f\infty_1\infty_2$ where f is the index of $\mathcal{O}$ and ∞_1, ∞_2 are the two infinite primes. Because our forms are indefinite there are two distinct Archimedean valuations of $1 + \sqrt{n}$ which account for two embeddings in $\mathbb{R}$ and therefore the two infinite primes. In the complex case there are two archimedian embeddings as well but they give rise to the same valuation.

$$\text{Complex case: } K \to \mathbb{C} \to \mathbb{R}_{\geq 0}$$

$$\text{Real case: } K \rightrightarrows \mathbb{R} \to \mathbb{R}_{\geq 0}$$

There is an isomorphism between the narrow class group of $\mathcal{O}$ and the Galois group of H_f^+/K using the Artin symbol [6]. We will first examine the Artin Symbol before stating the isomorphism.

Theorem 4.1. *Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ that is unramified in L. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ dividing $\mathfrak{p}$, then there is a unique element $Frob_{L/K}(\mathfrak{P}) = \sigma \in Gal(L/K)$ such that for all $\alpha \in \mathcal{O}_L$*

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

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

For the Frobenius element of $\mathfrak{P}$ we have

$$\mathrm{Frob}_{L/K}(\sigma(\mathfrak{P})) = \sigma \mathrm{Frob}_{L/K}(\mathfrak{P})\sigma^{-1}$$

Thus, if L/K is abelian, the element is independent of the choice of a prime $\mathfrak{P}|\mathfrak{p}$ and we call it the Artin Symbol of $\mathfrak{p}$:

$$\mathrm{Art}_{L/K}(\mathfrak{p}) := \mathrm{Frob}_{L/K}(\mathfrak{P})$$

Now that we have some knowledge of the Artin symbol we can state the isomorphism.

Theorem 4.2. *Given an order $\mathcal{O}_f$ with field of fractions K the Galois group of the ring class field of $\mathcal{O}_f$, $Gal(H_f/K)$ is isomorphic to the class group of $\mathcal{O}_f$ by mapping primes of the class group to their Artin symbol.*

$$Cl^+(\mathcal{O}_f) \xrightarrow{\sim} Gal(H_f^+/K)$$

$$[\mathfrak{a}] \to Art_{H_f^+/K}(\mathfrak{a})$$

With this and the knowledge from the previous sections we can make the connection between a prime $p \nmid 4n$ being represented by $x^2 - ny^2$ of discriminant Δ and its splitting behaviour in the ring class field. We will do this using the set of steps shown below and explain them afterwards.

$$\begin{aligned}
&p = x^2 - ny^2 \\
&\Leftrightarrow \exists\ \alpha \in \mathbb{Z}[\sqrt{n}] : N(\alpha) = p \\
&\Leftrightarrow \exists\ \mathfrak{p} \subset \mathbb{Z}[\sqrt{n}] : N(\mathfrak{p}) = p \quad \& \quad \mathfrak{p} = (\pi) \text{ met } N(\pi) = p \\
&\Leftrightarrow \exists \quad \mathfrak{p}|p \quad [\mathfrak{p}] = 0 \in \mathrm{Cl}^+(\mathbb{Z}[\sqrt{n}]) \\
&\Leftrightarrow p = \mathfrak{p} \cdot \mathfrak{p}' \text{ in } K/\mathbb{Q} \text{ en } \mathrm{Art}_{H_f^+/K}(\mathfrak{p}) = \mathrm{id} \\
&\Leftrightarrow \text{p splits completely in } H_f^+/\mathbb{Q}
\end{aligned} \tag{4}$$

We have that $p = x^2 - ny^2$ if and only if there is an element with norm p in $\mathbb{Z}[\sqrt{n}]$. The second step follows because the element is also the generator of a principal ideal with norm p because p is a prime. In the class group all of these primes have to be in the identity class because they are principal and of positive norm which is the third step. The identity element of the narrow ideal class group maps to the identity in the Galois group giving us the fourth step. For the fifth step $p = \mathfrak{p}\mathfrak{p}'$ implies splitting in $K/\mathbb{Q}$ and having trivial Artin Symbol in H_f/K implies that $\mathfrak{p}$ splits completely in H_f/K. Which means $\mathfrak{p}$ splits completely in $H_f^+/\mathbb{Q}$ which proves

$$p = x^2 - ny^2 \Leftrightarrow p \text{ splits completely in } H_f/\mathbb{Q}$$

Now that we have answered our initial question of which primes are represented by $x^2 - ny^2$ the next question becomes what primes are represented by other forms of discriminant $\Delta = 4n$. We will now show that a prime $p \nmid 4n$ is represented by a form of discriminant $4n$ if and only if $\left(\frac{4n}{p}\right) = 1$. We will do this by showing that for each of those p there exists a form (p, b, c) of discriminant $4n$. Such a form needs to have discriminant $b^2 - 4pc = 4n$. Because of $\left(\frac{4n}{p}\right) = 1$ we can take b as $b^2 \equiv 4n \mod p$. We can take b to be even as if it is not we

simply take $b+p$ since p is odd. Now we have that b^2-4n is divisible by $4p$ as it is $0 \mod p$ and divisible by 4. Which means that there exists c such that $b^2-4n=4pc$. This form $f(x,y)=px^2+bxy+cy^2$ represents p as $f(1,0)=p$. The converse is also true[6, Thm 2.3, p. 23]. Notice that since b and $-b$ both satisfy the equation above there are two choices for the form representing p that are equivalent but not necessarily properly equivalent. As mentioned in section 2 these forms are each others inverses. In the case of x^2-ny^2 this did not matter as it is its own inverse. Forms of discriminant $\Delta=4n$ that represent p always have a single class in $\mathcal{F}_\Delta/\mathrm{GL}_2(\mathbb{Z})$ and have either 1 or 2 classes in $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$ depending on whether they are their own inverses.

5 Densities

As mentioned and demonstrated in section 1, we can say something about the densities of primes represented by our equations. We will now state a more precise theorem on densities and show the result from section one to be a special case of this theorem. The *Chebotarev Density Theorem*:

Theorem 5.1. *Let L be a Galois extension of K, and let $C(\sigma)$ be the conjugacy class of an element $\sigma \in Gal(L/K)$. Then the set*

$$\mathcal{S}=\{\mathfrak{p}\in\mathcal{P}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } Frob_{L/K}(\mathfrak{p})=C(\sigma)\}$$

has density

$$\delta(\mathcal{S})=\frac{|C(\sigma)|}{|Gal(L/K)|}=\frac{|C(\sigma)|}{[L:K]}$$

Proof. See Neukirch [12, Chapter V, Theorem 6.4] □

In our case the conjugacy classes are fairly easy to calculate. We can start with this short exact sequence:

$$1\to \mathrm{Gal}(H_f^+/K)\to \mathrm{Gal}(H_f^+/\mathbb{Q})\to \mathrm{Gal}(K/\mathbb{Q})\to 1$$

Here $\mathrm{Gal}(H_f^+/K)\cong \mathrm{Cl}^+(\mathcal{O}_f)$ is abelian, $\mathrm{Gal}(K/\mathbb{Q})=\langle\sigma_0\rangle\cong\mathbb{Z}/2\mathbb{Z}$ and the sequence splits so $\mathrm{Gal}(H_f^+/\mathbb{Q})\cong \mathrm{Cl}^+(\mathcal{O}_f)\rtimes\langle\sigma_0\rangle$. This is a generalized dihedral group as the action of σ_0 on $\mathrm{Gal}(H_f^+/\mathbb{Q})$ is inversion. Now we can state the following theorem about the densities of primes of binary quadratic forms:

Theorem 5.2. *The density of the primes represented by a form $f \in \mathcal{F}_\Delta$ is*

$$\frac{1}{[H_f^+ : \mathbb{Q}]} \text{ if } f^{-1} \text{ is properly equivalent to } f$$

and

$$\frac{2}{[H_f^+ : \mathbb{Q}]} \text{ if } f^{-1} \text{ is not properly equivalent to } f$$

Proof. As we stated above $\mathrm{Gal}(H_f^+/\mathbb{Q})$ is a generalized dihedral group. Therefore for all $\sigma \in \mathrm{Gal}(H_f^+/K)$ the only elements in $C(\sigma)$ are $\{\sigma, \sigma^{-1}\}$. Now in our case of number rings there are two possibilities, either $\sigma = \sigma^{-1}$ and $|C(\sigma)| = 1$ or $\sigma \neq \sigma^{-1}$ and $|C(\sigma)| = 2$. This implies that the density of primes of a form is either $\frac{1}{\#\mathrm{Gal}(H_f^+/\mathbb{Q})}$ if σ is its own inverse or $\frac{2}{\#\mathrm{Gal}(H_f^+/\mathbb{Q})}$ if its not. Being its own inverse in the Galois group is the same as having f^{-1} be properly equivalent to f by Theorems 3.1 and 4.2 □

Next we will show that Dirichlet density is a special case of the Cheboterov Density Theorem.

Corollary 5.3. *The congruence class* 1 *mod* $2m$ *contains* $\frac{1}{\varphi(2m)}$ *of all prime numbers.*

Proof. This corollary is a special case of Theorem 5.1. Being $1 \mod 2m$ is equivalent to splitting in $\mathbb{Q}(\zeta_{2m})$ and with the fact that $[\mathbb{Q}(\zeta_{2m}) : \mathbb{Q}] = \varphi(2m)$ we get the desired result. □

We note that the primes represented by all forms in $\mathcal{F}_\Delta$ are $\frac{1}{2}$ of all primes. This is because the condition for a prime to be represented by any form of a given discriminant is that that prime splits in the field $\mathbb{Q}(\sqrt{\Delta})$. And a prime splits in that field if and only if $\left(\frac{\Delta}{p}\right) = 1$ which is true for half of all primes by Theorem 1.2.

6 Examples

We will finish with a few examples in which we apply the theory. The first example $n = 321 = 3 \cdot 107$ is an easy one to warm up with a composite number that leads to a non trivial but small class group. This first example will also be done in more detail and mostly by hand. The second example $n = 369 = 3^2 \cdot 41$ contains a class group that gets bigger because of the conductor. The last example is $n = 154305 = 3^5 \cdot 5 \cdot 127$. The class group doesn't get all that big because for real quadratic extensions the class group stays a lot smaller than in the complex case.

Before we get into the examples we will first go over a useful exact sequence:

$$1 \to (\mathcal{O}_K/f\mathcal{O}_K)^* \,/\, (\mathbb{Z}/f\mathbb{Z})^* \cdot im\ \mathcal{O}_K^* \to Cl^+(\mathcal{O}) \to Cl^+(\mathcal{O}_K) \to 1$$

Here we see the difference between the narrow class group of the maximal order and the narrow class group of the order we are interested in. Here $\mathfrak{f} = f \cdot \infty_1\infty_2$ is the conductor including the infinite primes. We see that the kernel of the map is exactly the ideals that become principal in the narrow class group of the maximal order.

Example 6.1. To solve our question for $p = x^2 - 321y^2$ we have to look at the order $\mathcal{O} = \mathbb{Z}[\sqrt{321}]$. We find that $\mathcal{O}$ is not the maximal order and that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{321}}{2}]$ is. The fundamental unit in both orders is $12\sqrt{321}+215$ as calculated using SAGE. The $\mathcal{F}_\Delta/\mathrm{PSL}_2(\mathbb{Z})$ has cardinality 6, so $\mathrm{Gal}(H_f^+/K)$ also has cardinality 6. For this one example we will show the entire form class group separated in cycles calculated using a small SAGE script:

$$F_1 = [(-32, 30, 3), (3, 30, -32), (-32, 34, 1), (1, 34, -32)]$$

$$F_2 = [(-25, 22, 8), (8, 26, -19), (-19, 12, 15), (15, 18, -16), (-16, 14, 17), (17, 20, -13), (-13, 32, 5), (5, 28, -25)]$$

$$F_3 = [(-25, 28, 5), (5, 32, -13), (-13, 20, 17), (17, 14, -16), (-16, 18, 15), (15, 12, -19), (-19, 26, 8), (8, 22, -25)]$$

$$F_4 = [(-17, 14, 16), (16, 18, -15), (-15, 12, 19), (19, 26, -8), (-8, 22, 25), (25, 28, -5), (-5, 32, 13), (13, 20, -17)]$$

$$F_5 = [(-17, 20, 13), (13, 32, -5), (-5, 28, 25), (25, 22, -8), (-8, 26, 19), (19, 12, -15), (-15, 18, 16), (16, 14, -17)]$$

$$F_6 = [(-3, 30, 32), (32, 34, -1), (-1, 34, 32), (32, 30, -3)]$$

Now we can use that $321 \equiv 1 \mod 8$ to get that 2 splits in $\mathcal{O}_K$ and $(\mathcal{O}_K/2\mathcal{O}_K)^* = \mathbb{F}_2^* \times \mathbb{F}_2^*$. Which in turn implies that the first part of the exact sequence mentioned at the start,

$$(\mathcal{O}_K/f\mathcal{O}_K)^* \,/\, (\mathbb{Z}/f\mathbb{Z})^* \cdot im\ \mathcal{O}_K^*\ ,$$

is trivial. The first part of the exact sequence being trivial means that the narrow class group of the maximal order is equal to the narrow class group of $\mathcal{O}$. Since we have already calculated the form class group we know that the narrow class group has order 6 as well.
We do not have a unit of norm -1 so the narrow class group is twice as big as the regular class group, which lines up nicely with the form class group being of cardinality 6. Now we need to find an order 2 extension. Luckily we can get it cheaply from the genus field. We can extend the field of fractions by $\sqrt{-3}$ to get an abelian extension unramified at all finite primes. Since it ramified at infinity it wasn't part of the Hilbert class field. This, as an extension of the Hilbert class field of $\mathcal{O}_K$, makes up for the entire ring class field as the Galois group of these two extensions is of order 6 as shown in figure 4. The Hilbert class

field can be hard to find, there is an algorithm but it is slow as the input becomes larger. In this case it is more than small enough and we can simply get the answer using SAGE. . Therefore we know that the Hilbert class field is $K(\beta)$ with β the root of $X^3 - X^2 - 4X + 1$.

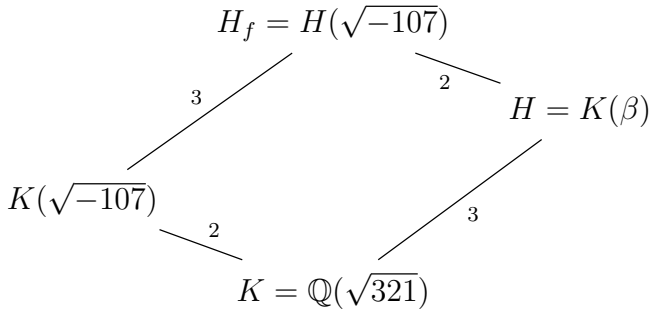


Figure 4: Field diagram of all subfields of the ring class field over K

Now that we have the class group, generated by the prime $[\mathfrak{p}_2]$ lying over 2, and the narrow classgroup, also generated by $[\mathfrak{p}_2]$, we will create a diagram with equations, ideals and elements of the Galois group that are mapped to each other down below. We know F_1, as seen in the cycles of forms, is the identity because it contains $a = 1$. We know F_6 is $[\mathfrak{p}_2]^3$ because it contains $a = -1$. In the form class group we can see that 5 is represented by F_2 and F_3 and -5 by F_4 and F_5.

The next question is which classes in the narrow ideal class group contain $\mathfrak{p}_5, \mathfrak{q}_5$, the primes laying over 5, hence we apply our map from the form class group to the narrow ideal class group. This sends $(5, 28, -25)$ to $\mathbb{Z} \cdot 5 + \mathbb{Z} \cdot (-14 + \sqrt{321})$ which is $(5, \sqrt{321} + 1) \in \mathcal{O}$ and then $(5, \alpha) \in \mathcal{O}_K = \mathbb{Z}[\alpha]$, giving us that F_2 maps to $\mathfrak{q}_5$. When we look at (α) we see that $\alpha = \mathfrak{q}_2^4\mathfrak{q}_5$ is principal and therefore $\mathfrak{q}_5$ is in the same class as $\mathfrak{p}_2$.We can place the final two form cycles because $(5, 28, -25)$ composed with a form from F_6 should land in the same cycle as $(-5, 28, 25)$. This follows, naturally, because F_6 is the class where we find principal ideals that aren't positively generated. We find that F_2 and F_6 combine to F_5 which is then in the class of $\mathfrak{p}_2^4$:

0	$[\mathfrak{p}_2]$	$[\mathfrak{p}_2]^2$	$[\mathfrak{p}_2]^3$	$[\mathfrak{p}_2]^4$	$[\mathfrak{p}_2]^5$
$p = x^2 - ny^2$	F_2	F_4	$-p = x^2 - ny^2$	F_5	F_3
	$\mathfrak{q}_5$		$(\sqrt{321})$		
id	$\sigma\rho$	ρ^2	σ	ρ	$\sigma\rho^2$

The final line is the identification of both class and form class group elements with elements

of the Galois group of the ring class field:

$$Gal(H_f/K) = \langle\ \sigma^2 = \rho^3 = id \mid \sigma\rho = \rho\sigma\ \rangle$$

Now to see for which p there exist x, y such that $p = x^2 - 321y^2$ we only need to know where p belongs in the table above. To see which forms represent $-p$ we take the form that represents p and take the composite with F_3. Of course instead of taking the composite we can also do the same calculation in the narrow ideal class group by adding the class containing $\mathfrak{p}$ the prime over p and the class $[\mathfrak{p}_2^3]$. For the total picture we get that p is represented by a form in a cycle if:

$$F_1, \left(\frac{321}{p}\right) = 1, \left(\frac{-3}{p}\right) = 1 \text{ and } X^3 + X^2 - 4X - 1 \text{ splits completely}$$

$$F_2, F_3, \left(\frac{321}{p}\right) = 1, \left(\frac{-3}{p}\right) \neq 1 \text{ and } X^3 + X^2 - 4X - 1 \text{ does not split completely}$$

$$F_4, F_5, \left(\frac{321}{p}\right) = 1, \left(\frac{-3}{p}\right) = 1 \text{ and } X^3 + X^2 - 4X - 1 \text{ does not split completely}$$

$$F_6, \left(\frac{321}{p}\right) = 1, \left(\frac{-3}{p}\right) \neq 1 \text{ and } X^3 + X^2 - 4X - 1 \text{ splits completely}$$

By the density theorem we have that F_1 and F_6 both represent $\frac{1}{12}$ of all primes, F_2, F_3 represent $\frac{1}{6}$ of the primes and F_4, F_5 represent $\frac{1}{6}$ of the primes. With none of these having overlap outside of their inverse. Note that half of all primes are represented by forms of discriminant $4 \cdot 321$. △

Example 6.2. For $p = x^2 - 369y^2$ we have to look at the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{369}] = \mathbb{Z}[6\left(\frac{1+\sqrt{41}}{2}\right)]$. The regular class group is trivial. The difference between the narrow and regular class group only depends on the existence of a unit of norm -1 in $\mathcal{O}$. There is a fundamental unit ϵ of norm -1 in $\mathcal{O}_K$. To get that unit into $\mathcal{O}$ we need a fourth power, making the norm positive. We conclude that the narrow class group of $\mathcal{O}$ is twice as big as the class group of $\mathcal{O}$. We can verify the size of the narrow class group using the exact sequence mentioned at the start of this section:

$$1 \to (\mathcal{O}_K/\mathfrak{f}\mathcal{O}_K)^* \,/\, (\mathbb{Z}/6\mathbb{Z})^* \cdot im\ \mathcal{O}_K^* \to Cl^+(6^2 \cdot 41) \to Cl^+(41) \to 1$$

Here $\mathfrak{f} = 6f_\infty f'_\infty$ is the conductor including the infinite primes. Then by definition we have $(\mathcal{O}_K/\mathfrak{f}\mathcal{O}_K)^* = (\mathcal{O}_K/f\mathcal{O}_K)^* \times \langle -1\rangle \times \langle -1\rangle$. We can split $(\mathcal{O}_K/6\mathcal{O}_K)^*$ into $(\mathcal{O}_K/2\mathcal{O}_K)^* \times (\mathcal{O}_K/3\mathcal{O}_K)^*$. Since $321 \equiv 1 \mod 8$ we have $(\mathcal{O}_K/2\mathcal{O}_K)^* \cong \mathbb{F}_2^*$ which is the trivial group.

The other group $(\mathcal{O}_K/3\mathcal{O}_K)^*$ is $\mathbb{F}_9^*$ as 3 is inert. Then in the quotient we have $(\mathbb{Z}/6\mathbb{Z})^* = \mathbb{F}_3^*$ and $\langle\epsilon_{41}\rangle \cdot \langle -1\rangle$ which is $\frac{5}{3}\sqrt{369} - 32$ with $\epsilon_{41}^4 \in \mathcal{O}$, which leaves a group of order 2.
The ring class field luckily isn't hard to find, in the exact sequence we can already see that the prime 2 in the conductor is trivial, so we expect ramification at 3 and infinity. This would mean adding $\sqrt{-3}$ as this is unramified and in the narrow genus field (the genus field where we allow ramification at infinity). This leads to the conclusion that $p = x^2 - 369y^2$ if $\left(\frac{369}{p}\right) = 1$ and $\left(\frac{-3}{p}\right) = 1$. The other class is for the negative p, so $-p = x^2 - ny^2$ if $\left(\frac{369}{p}\right) = 1$ and $\left(\frac{-3}{p}\right) \neq 1$. △

Example 6.3. As a final example we will look at $p = x^2 - 154305y^2$ with $154305 = 9^2 \cdot 1905 = 9^2 \cdot 5 \cdot 3 \cdot 127$. We need the ring class field of the order $\mathbb{Z}[\sqrt{154305}]$ which is an order of index 18 in the maximal order $\mathbb{Z}[\frac{1+\sqrt{1905}}{2}]$. The minimal polynomial of α, the generator of the maximal order, is $X^2 - X - 476$. The Minkowski bound rounded down to the nearest prime is 19 so there is quite some ground to cover. We first list the splitting behavior of primes up to 19.

$$\begin{aligned}
(2) &= (2, \alpha+1)(2, \alpha) && = \mathfrak{p}_2\mathfrak{q}_2 \\
(3) &= (3, \alpha+1)^2 && = \mathfrak{p}_3^2 \\
(5) &= (5, \alpha+2)^2 && = \mathfrak{p}_5^2 \\
(7) &= (7, \alpha)(7, \alpha-1) && = \mathfrak{p}_7\mathfrak{q}_7 \\
(11) &= (11) \\
(13) &= (13) \\
(17) &= (17, \alpha)(17, \alpha-1) && = \mathfrak{p}_{17}\mathfrak{q}_{17} \\
(19) &= (19, \alpha+4)(19, \alpha+14) && = \mathfrak{p}_{19}\mathfrak{q}_{19}
\end{aligned}$$

Now we can find relations to get the class group of the maximal order. As in example 6.1 we will try some values to get relations in the class group as shown in the table below.

k	20	21	22	23	24	25	26	30	34	35
$f(k)$	-96	-56	-14	30	76	124	174	394	646	714
$(k-a)$	$\mathfrak{q}_2^5\mathfrak{p}_3$	$\mathfrak{p}_2^3\mathfrak{p}_7$	$\mathfrak{q}_2\mathfrak{q}_7$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	$\mathfrak{q}_2\mathfrak{q}_{19}$	$\mathfrak{p}_2\mathfrak{p}_{31}$	$\mathfrak{q}_2\mathfrak{p}_3\mathfrak{p}_{29}$	$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{q}_7$	$\mathfrak{q}_2\mathfrak{p}_{17}\mathfrak{p}_{19}$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7\mathfrak{q}_{17}$

Table 1: Simple relations in the class group

Combining 21 and 22 we get that $\mathfrak{p}_2^2$ is principal just like $\mathfrak{p}_7$. Using 20 we get that $\mathfrak{p}_3$ is in the same class as $\mathfrak{p}_2$. Then $k = 23$ tells us that $\mathfrak{p}_5$ is principal. By $k = 24$ we have that $\mathfrak{q}_{19}$ is in

the same class as $\mathfrak{q}_2$ and then by $k = 34$ we get that $\mathfrak{p}_{17}$ is principal. The only question that remains is whether $\mathfrak{p}_2$ is principal or of order 2. Since we know that the genus field contains $\sqrt{5}$ it has to be order 2.

We conclude that the class group of the maximal order is generated by $\mathfrak{p}_2$ and of order 2. Calculating the form class group of the order $\mathcal{O}$ we find that it has cardinality 12 and thus the narrow class group also has cardinality 12.

With ramification at infinity the genus field also gets $\sqrt{-3}$ and implicitly $\sqrt{-127}$. The extensions so far are $K(\sqrt{-3}, \sqrt{5})$ which make for a degree 4 extension. Since the Galois group of H_f^+/K is of order 12 we still need to find some degree 3 extension. This is added by the index 9 in our order. As we know that in the local case wild ramification is given by Eisenstein polynomials we go looking for an Eisenstein polynomial with discriminant $9^2 \cdot 4 \cdot 1905$ by asking our computer to try random eisenstein polynomials of degree 3 and find $X^3 - 18X^2 + 45X - 15$. Adding the zeroes of $X^3 - 18X^2 + 45X - 15$, $\sqrt{5}$ and $\sqrt{-3}$ we get the ring class field. From there finding the splitting conditions and corresponding forms can be done in the same way as example 1. Finally we find:

$$p = x^2 - 154305y^2 \Leftrightarrow \left(\frac{154305}{p}\right) = 1, \left(\frac{-3}{p}\right), \left(\frac{5}{p}\right) = 1 \text{ and}$$

$$X^3 - 18X^2 + 45X - 15 \text{ splits completely mod } p$$

We find that this is correct for the primes below 100 with the only solution $p = 79$ for $x = -737345292069504821812383022930718528$ and $y = 18770719167976981611060023826899 59$ there is of course infinitely many x, y for which this is true but this is just one example. It turns out that the only other prime below 1000 that is represented is 199. This is against the odds as we would expect $\frac{1}{24}$ primes to be represented and there are 168 primes below 1000. This is however not unthinkable. △

References

[1] Leonhard Euler. *Leonhard Euler Opera Omnia / Series prima: Opera mathematica*. Birkhäuser Basel, 1992.

[2] Joseph Louis Lagrange. *Oeuvres*. Vol. 3. Paris: Gauthier-Villars, 1869.

[3] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Leipzig, 1801.

[4] E.E. Kummer. "Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren". In: *Jour. für Math. (Crelle)* 35 (1847), pp. 327–367.

[5] Peter Gustav Lejeune Dirichlet and Richard Dedekind. *Lectures on number theory*. 16. American Mathematical Soc., 1999.

[6] David A. Cox. *Primes of the Form $x^2 + ny^2$*. 2nd ed. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs, and Tracts. Wiley, 2013.

[7] PG Lejeune Dirichlet. "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält". In: *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften* 45 (1837), p. 81.

[8] Atle Selberg. "An elementary proof of Dirichlet's theorem about primes in an arithmetic progression". In: *Annals of Mathematics* (1949), pp. 297–304.

[9] Peter Gustav Lejeune Dirichlet. *Zahlentheorie*. 4th ed. Vieweg, Braunschweig, 1894.

[10] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[11] H.W. Lenstra. "On the calculation of regulators and class numbers of quadratic fields". In: *Journées Arithmétiques 1980, London Math. Soc. Lecture Note Ser. 56* (1982), pp. 123–150.

[12] Jürgen Neukirch. *Class field theory*. Vol. 280. Springer, 1986.