# QUANTUM ALGORITHM FOR SOLVING PELL'S EQUATION

YOUNG JIN KIM

Contents



## 1. Introduction

Let $x, y \in \mathbb{N}$. The Diophantine equation

$$x^2 - dy^2 = 1$$

for some $d \in \mathbb{N}$ that is square free is called *Pell's equation*, which has been a problem for thousands of years. This equation was conjectured to have an infinite number of solutions by Fermat in the 1600s and this was eventually solved by Lagrange. More interestingly,

there is exactly one positive solution such that every other solution is a power of that one solution up to sign, which is called the *fundamental unit*. In this writeup, we will try to address the mathematics going behind the ideas for a quantum algorithm that would provide the value for the natural logarithm of the fundamental unit, which we call the *regulator*. That is, much of this writeup will be devoted for the interested reader to be able to be prepared to read the algorithm given by Hallgren, who provided a quantum algorithm that solves for the regulator quite efficiently.

## 2. Algebraic Numbers and Integers

A complex number $\alpha$ is an *algebraic number* if $\alpha$ is the root of some monic polynomial with rational coefficients,

$$p(\alpha) = 0, \quad p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \quad c_i \in \mathbb{Q}.$$

We note that every rational number $q \in \mathbb{Q}$ is algebraic since it satisfies the polynomial $(x - q)$, but not every algebraic number is rational, such as $(1 + \sqrt{5})/2$, which is a root of the polynomial $x^2 - x - 1$. The set of all algebraic numbers is denoted as $\overline{\mathbb{Q}}$.

**Theorem 2.1.** *Let $\alpha \in \mathbb{C}$. The following are equivalent:*

*(1) $\alpha$ is an algebraic number, i.e., $\alpha \in \overline{\mathbb{Q}}$.*
*(2) The ring $\mathbb{Q}[\alpha]$ is a finite dimensional vector space over $\mathbb{Q}$.*
*(3) $\alpha$ belongs to a ring $R$ in $\mathbb{C}$ that is also a finite dimensional $\mathbb{Q}$-vector space.*

*Proof.* Let us first show that the first statement implies the second. Let $\alpha$ be the root of a monic polynomial with rational coefficients $p(x) \in \mathbb{Q}[x]$ where
$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Since $\alpha$ is a root, it follows that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \Longrightarrow \alpha^n = -\sum_{i=1}^{n-1} a_i x^i,$$

giving us that the finite dimensional vector space generated by $\{1, \alpha, \ldots, \alpha^{n-1}\}$ also contains $\alpha^n$. We now proceed by induction on $n$ and show that $\alpha^{n+1}$ is also generated by the finite set of generators $\{1, \alpha, \ldots, \alpha^{n-1}\}$ over $\mathbb{Q}$. Since $\alpha^n$ is in this set, and by the equation above, we get that

$$\alpha^{n+1} + a_{n-1}\alpha^n + \cdots + a_1\alpha^2 + a_0\alpha = 0 \Longrightarrow \alpha^{n+1} = -\sum_{i=1}^{n-1} a_i x^{i+1},$$

giving us that $\alpha^{n+1}$ is generated. By induction, this holds for all higher powers of $\alpha$, proving the first implication.

Suppose the ring $\mathbb{Q}[\alpha]$ is a finite dimensional vector space over $\mathbb{Q}$. Since $\alpha \in \mathbb{Q}[\alpha]$, we have shown that the second statement implies the third.

Now suppose the third statement. We will show that this implies the first statement. Since the ring $R$ can be viewed as a finite dimensional vector space over $\mathbb{Q}$, let $\{r_1, \ldots, r_n\}$ form a basis of $R$ as a $\mathbb{Q}$-vector space. Scaling each of the basis vectors by $\alpha$, we get a linear combination for $\alpha r_i$ for all $i$, i.e.,

$$\alpha r_i = \sum_{i=1}^{n} a_{ij} r_j, \quad \text{for } i = 1, \ldots, n.$$

So if we let $A$ be the matrix given by $A_{ij} = a_{ij} \in \mathbb{Q}^{n \times n}$, we can rewrite the equation above as

$$\alpha \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = A \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

giving us that $\alpha$ is an eigenvalue of $A$ and therefore satisfying the characteristic polynomial of $A$, giving us our desired results. □

This theorem leads us to the following result:

**Corollary 2.2.** *The algebraic numbers $\overline{\mathbb{Q}}$ form a field.*

*Proof.* Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then by the theorem, we get that the rings $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ are finite dimensional vector spaces with bases given by $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ and $\left\{1, \beta, \ldots, \beta^{m-1}\right\}$, respectively. Consider the ring $R = \mathbb{Q}[\alpha, \beta]$. As a $\mathbb{Q}$-vector space, we get that a basis is given by

$$\left\{\alpha^i \beta^j : 0 \leq i \leq n, 0 \leq j \leq m\right\}$$

and so it is clear from this that $\alpha + \beta,\ \alpha\beta \in \overline{\mathbb{Q}}$.

Finally, we now need to show that multiplicative inverses exist, so suppose $\alpha \neq 0$. Since $\alpha \neq 0$, without loss of generality, we can assume that the monic polynomial $\alpha$ satisfies has a nonzero constant term $a_0$ since otherwise we can factor out the lowest power of $x$ in the polynomial. The relation $p(\alpha) = 0$ can be rewritten to be

$$\alpha^{-1} = -\frac{p(\alpha) - a_0}{a_0 \alpha} \in \mathbb{Q}[\alpha]$$

and so by the third condition of the theorem, we conclude that $\alpha^{-1}$ is algebraic, giving us a field structure for $\overline{\mathbb{Q}}$. □

**Remark.** The algebraic numbers are the algebraic closure of $\mathbb{Q}$. We highlight this to say that the closure symbol for the algebraic numbers is justified, and that $\mathbb{C}$ is the more familiar algebraic closure of $\mathbb{R}$. We do not prove these statements here though since we will not be using these facts.

We can retell this entire story by specializing to the case of looking at monic polynomials in $\mathbb{Z}[x]$. That is, a complex number $\alpha$ is an *algebraic integer* if $\alpha$ is the root of some monic polynomial with integer coefficients,

$$p(\alpha) = 0, \quad p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \quad c_i \in \mathbb{Z}.$$

The set of all algebraic integers are denoted as $\overline{\mathbb{Z}}$. Just as before, every integer $n \in \mathbb{Z}$ is an algebraic integer since it satisfies the monic polynomial $(x - n)$, but the converse is not true. For example, we still have $(1 + \sqrt{5})/2$ to be an algebraic integer, despite not even being rational, since it is the root of the monic polynomial $x^2 - x - 1$.

In a similar manner, we have the following results:

**Theorem 2.3.** *Let $\alpha \in \mathbb{C}$. The following are equivalent:*

*(1) $\alpha$ is an algebraic integer, i.e., $\alpha \in \overline{\mathbb{Z}}$.*
*(2) The ring $\mathbb{Z}[\alpha]$ is a finite generated $\mathbb{Z}$-module.*
*(3) $\alpha$ belongs to a ring $R$ in $\mathbb{C}$ that is also a finitely generated $\mathbb{Z}$-module.*

**Corollary 2.4.** *The set of algebraic integers forms a commutative ring.*

**Corollary 2.5.** *The algebraic integers are integrally closed, i.e., every monic polynomial in $\overline{\mathbb{Z}}[x]$ can be rewritten as a factor of linear terms and all of the roots are in $\overline{\mathbb{Z}}$*

We do not prove these statements since they are almost identical for the case of algebraic numbers and $\mathbb{Q}$-vector spaces. We note that the only difference is that for the arguments for the algebraic integers, we use the ring $\mathbb{Z}$, forcing us to work with $\mathbb{Z}$-modules instead of $\mathbb{Q}$-vector spaces and so the concept of "finite dimensionality" is generalized to the notion of "finitely generated".

For more fluency in going in between examples, we introduce the idea of a number field: A *number field* is a field $\Bbbk \subseteq \overline{\mathbb{Q}}$ such that the degree $[\Bbbk : \mathbb{Q}] = \dim_{\mathbb{Q}}(\Bbbk)$ is finite. In a number field $\Bbbk \subseteq \overline{\mathbb{Q}}$, the *number ring* or *ring of integers* of $\Bbbk$ is the ring of algebraic integers in $\Bbbk$,

$$\mathcal{O}_{\Bbbk} = \overline{\mathbb{Z}} \cap \Bbbk.$$

To get a first handle on these definitions, we go through a basic example.

**Proposition 2.6.** *Consider $\mathbb{Q}$ to be its own number field. The ring of integers in $\mathbb{Q}$ is simply $\mathbb{Z}$.*

*Proof.* Suppose $q \in \mathbb{Q}$ and is also an algebraic integer. Thus, $q$ must satisfy some monic polynomial $p(x)$, say of degree $n$. Since $q$ is rational, rewrite it as $a/b$ where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. This gives us that

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0$$

and clearing the denominators gives us

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0,$$

showing us that $b$ divides $a^n$. However, since $\gcd(a, b) = 1$ and $b|a^n$, we conclude that $b = \pm 1$. □

## 3. Quadratic Number Fields

An integer $d$ is said to be *square free* if $d$ is not the square of any integer, i.e., there is no $m \in \mathbb{Z}$ such that $d = m^2$.

We will now be studying the number fields $F$ with the property that $[F : \mathbb{Q}] = 2$, which we call *quadratic number fields*. Since $F$ is a degree 2 extension of $\mathbb{Q}$, we get that $F = \mathbb{Q}(\alpha)$ where $\alpha$ satisfies the quadratic equation $ax^2 + bx + c = 0$ for $a, b, c \in \mathbb{Z}$. By the infamous quadratic formula, we get that

$$\alpha = \frac{-b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

and so it is quite clear that $F = \mathbb{Q}\left(\sqrt{b^2 - 4ac}\right)$. If we rewrite $\sqrt{b^2 - 4ac} = m^2 d$, where $m, d \in \mathbb{Z}$ and $d$ is a square free integer, we get that $F = \mathbb{Q}(\sqrt{d})$ and so we get that a quadratic number field must be of the form

$$F = \mathbb{Q}(\sqrt{d}) = \left\{ a + b\sqrt{d} : a, b \in \mathbb{Q} \right\}$$

under the standard addition and multiplication operations, acting much like the Gaussian rationals. If $d$ is positive, then we say that the quadratic number field is *real*. If $d$ is negative, then the field is said to be *imaginary*. However, we will be mostly focused on the real quadratic case to address Pell's equation.

In a very similar manner to the Gaussian rationals, given an $\alpha = a + b\sqrt{d}$, define the *conjugate* of $\alpha$ to be $\overline{\alpha} = a - b\sqrt{d}$. Since $d$ is square free, we can conclude that

$$a + b\sqrt{d} = a' + b'\sqrt{d} \iff a = a' \text{ and } b = b'$$

giving us that the conjugation is a well defined operation. Thus, we can rephrase Pell's equation to be

$$\alpha\overline{\alpha} = 1, \quad \text{where } \alpha = a + b\sqrt{d}.$$

We now also define two functions relating $F$ with $\mathbb{Q}$. The *trace function* of $F$ is

$$\begin{aligned} \mathrm{tr} : F &\longrightarrow \mathbb{Q} \\ \alpha &\longmapsto \alpha + \overline{\alpha} \end{aligned}$$

and the *norm* of $F$ is

$$\begin{aligned} N : F^\times &\longrightarrow \mathbb{Q}^\times \\ \alpha &\longmapsto \alpha\overline{\alpha}. \end{aligned}$$

Thus, if $\alpha = a + b\sqrt{d}$, we get that $\mathrm{tr}(\alpha) = 2a$ and $N(\alpha) = a^2 - b^2 d$.

We can now quite concretely see what the ring of integers are for these quadratic fields.

**Proposition 3.1.** *The ring of integers of $F = \mathbb{Q}(\sqrt{d})$ are of the form*

$$\mathcal{O}_F = \mathbb{Z}[\omega] = \{m + n\omega : m, n \in \mathbb{Z}\}, \quad \textit{where } \omega = \begin{cases} \dfrac{-1+\sqrt{d}}{2} & \textit{if } d \equiv 1 \bmod 4 \\ \sqrt{d} & \textit{if } d \equiv 2, 3 \bmod 4 \end{cases}.$$

*Proof.* Suppose $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. We note that $\alpha \in \mathcal{O}_F$ if and only if $\mathrm{tr}(\alpha), N(\alpha) \in \mathbb{Z}$; this is because if $\alpha$ is an algebraic integer, then so is its conjugate $\overline{\alpha}$ since they both satisfy the same polynomial

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - \mathrm{tr}(\alpha) + N(\alpha),$$

and so the trace and the norm must be algebraic integers since they are defined to be the sum and product of algebraic integers, but they are also ordinary integers since they evaluate to $\mathbb{Q}$.

So suppose $\alpha = a + b\sqrt{d} \in \mathcal{O}_F$. Since $2a \in \mathbb{Z}$, we see that $4N(\alpha) = (2a)^2 - 4b^2 d$, giving us that $4b^2 d \in \mathbb{Z}$ as well. Writing $b = r/s$, where $\gcd(r, s) = 1$, any prime $p > 2$ dividing $s$ will result in $p^2 | d$, thus by the square-freeness of $d$, we conclude that $s \in \{\pm 1, \pm 2\}$. Thus, we get that $2b \in \mathbb{Z}$. Writing $m = 2a$ and $n = 2b$, we see that the condition $N(\alpha) \in \mathbb{Z}$ gives us that $m^2 - dn^2 \in 4\mathbb{Z}$. Recall that for all $x \in \mathbb{Z}/4\mathbb{Z}$ that $x^2 = 0, 1 \in \mathbb{Z}/4\mathbb{Z}$.

Thus, if $d \equiv 1$, then $m^2 - dn^2 \equiv m^2 - n^2 \bmod 4$. We note that $m^2 - n^2 \equiv 0$ if and only if they are of the same parity, and thus $\alpha \in \mathcal{O}_F$ must be of the form $\alpha = m + n\sqrt{d}$ where $m \equiv n \bmod 2$. Since $m \equiv 2 \bmod 2$, we get that $(m + n)/2 \in \mathbb{Z}$ and so writing

$$\frac{m + n\sqrt{d}}{2} = \frac{m + n}{2} + n\left(\frac{-1 + \sqrt{d}}{2}\right)$$

shows that $\mathcal{O}_F \subseteq \mathbb{Z} + \mathbb{Z}((-1 + \sqrt{d})/2)$. For the reverse containment, we note that since $d \equiv 1 \bmod 4$ that we can use the expression above to show that $(-1 + \sqrt{d})/2 \in \mathcal{O}_F$.

Now if $d \equiv 2, 3 \bmod 4$, then we have that $m^2 - dn^2 \equiv m^2 + 2n^2$ or $m^2 + n^2 \bmod 4$. Thus, for these to live in $4\mathbb{Z}$, we have that $m, n \in 2\mathbb{Z}$ and this gives us that $a, b \in \mathbb{Z}$, giving us our desired result. □

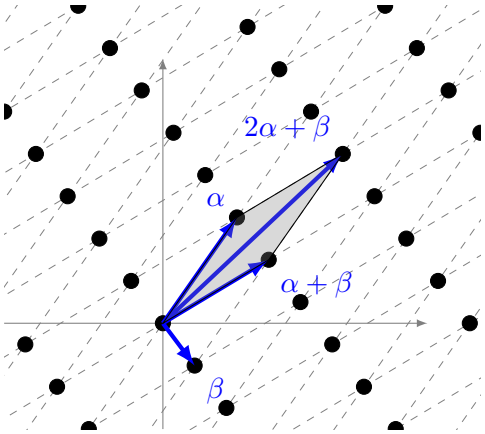



FIGURE 1. A lattice generated by algebraic integers $\alpha, \beta \in \mathcal{O}_F$

This result allows us to be able to view $\mathcal{O}_F$ as a finitely generated $\mathbb{Z}$-module with generators given by $\{1, \omega\}$, where $\omega$ is defined as above. That is, we can view $\mathcal{O}_F$ as a vector space over $\mathbb{Z}$ and this provides us with a geometric picture of a lattice (see Figure 1 below). More concretely, a pair $\alpha, \beta \in \mathcal{O}_F$ is called an *integral basis* if

$$\mathcal{O}_F = \alpha\mathbb{Z} + \beta\mathbb{Z} = \{\alpha m + \beta n : m, n \in \mathbb{Z}\}.$$

Thus, the pair above $\{1, \omega\}$ is an integral basis, but this choice is not unique to a lattice. However, a change of integral bases must preserve the fact that the coefficients are still integers to preserve the shape of the lattice.

This leads us the following lemma:

**Lemma 3.2.** *Let $\{\alpha, \beta\}$ be integral bases for $\mathcal{O}_F$. A pair of elements $\{\alpha', \beta'\}$ is another integral basis if and only if*

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad \textit{for some } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \{\pm I\}\,\mathrm{SL}_2(\mathbb{Z}).$$

*Proof.* Suppose we have two integral bases for $\mathcal{O}_F$. Since $\alpha', \beta' \in \mathcal{O}_F$, we get that $\alpha' = \alpha a + b\beta$ and $\beta' = \alpha c + d\beta$ for some $a, b, c, d \in \mathbb{Z}$. This gives us that

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \underbrace{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}_{\text{call } A} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

where $\det(A) = ad - bc \neq 0$, since otherwise $\{\alpha', \beta'\}$ would fail to generate $\mathcal{O}_F$. Thus, multiplying the equation on the left by $A^{-1}$ gives us expressions for $\alpha, \beta$ as integral linear combinations of $\{\alpha', \beta'\}$. However, since $A^{-1}$ must also have integral entries, we get that $\det(A) = \pm 1$.

Conversely, if we have a matrix $A \in \{\pm I\}\,\mathrm{SL}_2(\mathbb{Z})$, then both $\alpha\mathbb{Z} + \beta\mathbb{Z}$ and $\alpha'\mathbb{Z} + \beta'\mathbb{Z}$ are equal since the two sets $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$ can be expressed as integral linear combinations of each other. □

This proof, and result, can be generalized to cases that will arise later in the writeup, such as integral and fractional ideals of $\mathcal{O}_F$. This independence in the choice of basis leads us to an invariant of $F$.

**Proposition 3.3.** *For any integral basis $\{\alpha, \beta\}$ of $\mathcal{O}_F$, the determinant*

$$D_F = \det\left(\begin{bmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{bmatrix}\right)^2$$

*is a positive integer, independent of the choice of basis. This $D_F$ is called the* discriminant *of $F$. Moreover,*

$$D_F = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2, 3 \text{ mod } 4 \end{cases}.$$

*Proof.* Let $\{\alpha, \beta\}$ be an integral basis. Since we also know that $\{1, \omega\}$, where the value of $\omega$ is given in Proposition 3.1, is also an integral basis, we apply a change of integral basis matrix $A$ to get that

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix}^T = (A\begin{bmatrix}1\\ \omega\end{bmatrix})^T.$$

However, since the transpose does not change the determinant, this gives us that

$$\det\left(\begin{bmatrix}\alpha & \overline{\alpha}\\ \beta & \overline{\beta}\end{bmatrix}\right)^2 = \det\left(A\begin{bmatrix}1 & 1\\ \omega & \overline{\omega}\end{bmatrix}\right)^2 = \det(A)^2\det\left(\begin{bmatrix}1 & 1\\ \omega & \overline{\omega}\end{bmatrix}\right)^2 = \det\left(\begin{bmatrix}1 & 1\\ \omega & \overline{\omega}\end{bmatrix}\right)^2.$$

For the case of $d \equiv 1 \bmod 4$, we get that $D_F = d$ while for the case of $d \equiv 2, 3 \bmod 4$, we get that $D_F = 4d$. □

These cases allow us to provide a single description of the integers in terms of $D_F$ instead of $d$. Thus, we have

$$\mathcal{O}_F = \mathbb{Z}[r], \quad \text{where } r = \frac{D_F + \sqrt{D_F}}{2}.$$

3.1. **Units and the Fundamental Unit.** An algebraic integer $\alpha \in \mathcal{O}_F$ is called a *unit* if it has a multiplicative inverse that is also an algebraic integer. The *unit group* of $F$ is the multiplicative group $\mathcal{O}_F^\times$ consisting of all units of $\mathcal{O}_F$. For example, the units in the

algebraic integers of $\mathbb{Q}$, which we saw earlier is simply $\mathbb{Z}$, is only $\pm 1$. Thus the unit group of $\mathcal{O}_{\mathbb{Q}}^{\times} = \{\pm 1\}$.

**Proposition 3.4.** *An algebraic integer $\alpha \in \mathcal{O}_F$ is a unit if and only if $N(\alpha) = \pm 1$.*

*Proof.* Let $\alpha \in \mathcal{O}$ be a unit with its multiplicative inverse given by $\beta \in \mathcal{O}$. Thus, it follows that

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$$

and since both norms are integers, we conclude that $N(\alpha) = \pm 1$.

Conversely, suppose $N(\alpha) = \pm 1$. Now since

$$\alpha\overline{\alpha} = N(\alpha)$$

we get that $\pm\alpha\overline{\alpha} = \pm N(\alpha) = 1$ and so we get that $\pm\overline{\alpha}$ is the inverse for $\alpha$. □

**Proposition 3.5.** *Letting $\mathcal{O}_F$ be the ring of integers in $F = \mathbb{Q}(\sqrt{d})$ for $d > 0$, there exists a unique unit $u > 1$ such that every unit is of the form $\pm u^k$ where $k \in \mathbb{Z}$. More abstractly, there exists a unique $u \in \mathcal{O}_F^{\times}$ such that*

$$\mathcal{O}_F^{\times} = \{\pm 1\} \times \langle u \rangle.$$

*Proof.* We omit the proof here since it is not incredibly illuminating. For details, please see [IR13]. □

This unique unit is called the *fundamental unit* and denote it as $u_0$. Solving Pell's equation is equivalent to solving for the fundamental unit. However, these fundamental units can get exponentially large in input size as it is of the order $O(e^{\sqrt{d}})$. Thus, to get around this exponentially large sized numbers, we define the *regulator* to be $\ln u_0$ and study the regulator instead. The most efficient (classical) algorithm for solving the regulator has run time $O(e^{\sqrt{\log d}}\text{poly}(n))$ where $n$ denotes the number of digits of accuracy.

## 4. Studying Ideals of Algebraic Integers

Again, we let $F$ denote a quadratic number field and $\mathcal{O}_F$ to be ring of integers of $F$.

An *ideal* $\mathfrak{a}$ of $\mathcal{O}_F$ is a subset of $\mathcal{O}_F$ such that $\mathfrak{a}$ forms an additive abelian group and is closed under multiplication by $\mathcal{O}_F$, i.e., $\mathfrak{a}\mathcal{O}_F = \mathfrak{a}$. For example, the even integers in the ring $\mathbb{Z}$ forms an ideal since the sum or difference of any two even numbers is again even, and multiplication of any integer by an even number results in an even integer.

The *sum* of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal generated by the sums of the elements,

$$\mathfrak{a} + \mathfrak{b} = \{x + y : x \in \mathfrak{a},\ y \in \mathfrak{b}\}.$$

In a similar manner, the product of the two ideals is the ideal generated by the product of elements. To write this in set form, we note that due to the additive closure in ideals, we have to take the span of product of elements in the ideals,

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in \mathfrak{a},\ y_i \in \mathfrak{b},\ n \in \mathbb{N} \right\}.$$

A subset $I \subseteq F$ is a *fractional ideal* of $\mathcal{O}$ if there exists a nonzero $m \in F$ such that $mI \subseteq \mathcal{O}_F$ is an ideal.

To highlight the differences between an ideal (which we will call an integral ideal) and a fractional ideal, an ideal $\mathfrak{a}$, which we first defined at the beginning of the section, is a subset of $\mathcal{O}_F$, while a fractional ideal $I$ has the flexibility to be a subset of the number field $F$. Moreover, a fractional ideal is not closed under multiplication by elements of $F$. For example, if we considered the number field $\mathbb{Q}$ and its ring of integers $\mathbb{Z}$, then the abelian group generated by $(1/2)$ is a fractional ideal of $\mathbb{Z}$ since if we multiplied it by 2, we would get an ideal of $\mathbb{Z}$. However, if we multiplied elements in this group by $1/3$ for example, then we would get elements not in the group.

Just as we defined operations on integral ideals, we can also define multiplication for the fractional ideals. This is because if $I$ and $J$ are fractional ideals, then there are $\alpha, \beta \in F^\times$ such that $\alpha I$ and $\beta J$ are ideals of $\mathcal{O}_F$ and

$$(\alpha I)(\beta J) = \alpha\beta IJ.$$

We note that the multiplication is associative and commutative.

Just as any element $r$ in a ring $R$ can define a principal ideal by considering the set $(r) := rR = \{ra : a \in R\}$, every $x \in F^\times$ defines a fractional ideal by considering $(x) := x\mathcal{O}_F$. In a very similar fashion, fractional ideals of this form are called *principal*.

**Proposition 4.1.** *Let $(x), (y)$ be principal fractional ideals. Then*

$$(x) = (y) \iff x = yu, \text{ where } u \text{ is a unit in } F.$$

*Proof.* Suppose $(x) = (y)$. On one hand, since $x \in (x) = (y)$, we get that there exists a $z \in \mathcal{O}_F$ such that $x = yz$. On the other hand, since $y \in (y) = (x)$, we get that there exists a $z' \in \mathcal{O}_F$ such that $y = xz'$. This gives us that $x = xzz'$, and so we conclude that $z$ and $z'$ are units.

Conversely, suppose $x = yu$ for some unit $u \in F^\times$. Then it follows that

$$(x) = x\mathcal{O}_F = yu\mathcal{O}_F = y\mathcal{O}_F = (y),$$

giving us our desired result. □

Recall that the fundamental unit is the generator for the set of all units in $\mathcal{O}_F$, i.e., every unit $u = \pm u_0^k$ for some $k \in \mathbb{Z}$ where $u_0$ denotes the fundamental unit. This, combined with the previous proposition, allows us to convert our problem of computing the regulator into solving a periodicity problem. Indeed, let $(x)$ be a principal fractional ideal and see that

$$(x) = x\mathcal{O}_F = e^{\ln(x)}\mathcal{O}_F.$$

Letting $R = \ln(u_0)$ be the regulator of $\mathcal{O}_F$, we compute that

$$e^{\ln(x)+R}\mathcal{O} = e^{\ln(x)}\mathcal{O}_F$$

to see that $e^{\ln(x)}\mathcal{O}_F$ is a periodic function of $x$ with period $R$. However, since the binary representation of the fundamental unit is possibly exponential in $\log(D_F)$, no polynomial time algorithm for computing the fundamental unit exists. Since both $\mathbb{Q}(\sqrt{d})$ and $\mathcal{O}_F$ are dense in $\mathbb{R}$, to specify an ideal $x\mathcal{O}_F$ requires full precision of $x$. Alternatively, we can find a new framework where two ideals are effectively "almost identical". An idea was introduced by Gauss was to study *reduced* principal ideals and a notion of distance between ideals. This shrinks our infinitely large set of all fractional principal ideals to a finite set. Each reduced ideal, as we will see, will be $O(\text{poly}(\log(d)))$ bits and there will be only $O(d)$ number of them.

## 5. Reduction of Ideals

5.1. **Presentations of Ideals.** Let $\mathcal{P}(F)$ denote the set of all principal fractional ideals of $\mathcal{O}_F$. Before progressing, we quickly go through some presentations of fractional ideals.

**Proposition 5.1.** *A principal fractional ideal $I$ is of the form*

$$I = \alpha\mathbb{Z} + \beta\mathbb{Z} = \{\alpha n + \beta m : n, m \in \mathbb{Z}\}$$

*where $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ are linearly independent of each other.*

*Proof.* Since we know that $\mathcal{O}_F = \mathbb{Z} + \omega\mathbb{Z}$ where $\omega$ is defined as in Proposition 3.1, we can simply apply the change of integral basis as in Lemma 3.2. □

The $\alpha, \beta$ in the previous proposition are called the integral bases for the fractional ideal $I$. As we had noted earlier, the change of integral basis lemma, Lemma 3.2, works for fractional ideals and the proof is identical and is therefore not discussed here.

Now if $\{\alpha, \beta\}$ forms an integral basis for the fractional ideal $I$, then define the absolute value

$$\mathcal{N}(I) = \frac{1}{\sqrt{D_F}} \left| \det \begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} \right|.$$

**Proposition 5.2.** *The absolute value $\mathcal{N}(I)$ is independent of the choice of integral basis. Moreover, if $I = (x)$ is a principal integral ideal, then $\mathcal{N}(I) = N(x)$ where $N$ denotes the norm, as defined at the beginning of the writeup.*

*Proof.* Let $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$ be two different integral bases for the integral ideal $I$. By the change of integral bases, we have that there exists an invertible $2 \times 2$ matrix $A$ such that $\det(A) = \pm 1$ giving the relation

$$\underbrace{\begin{bmatrix} \alpha' & \beta' \\ \overline{\alpha'} & \overline{\beta} \end{bmatrix}}_{\text{call } X} = A \underbrace{\begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix}}_{\text{call } Y}$$

and since the determinant is multiplicative, and $\det(X) = \det(A)\det(Y) = \pm \det(Y)$, showing that $\mathcal{N}(I)$ is independent of the choice of basis.

Now, if $I = (x)$ is a principal integral ideal, taking $\alpha = x$ and $\beta = x(D_F + \sqrt{D})/2$ gives us that $\mathcal{N}(I) = |x\overline{x}|$, which of course is an integer for all $x \in \mathcal{O}_F$ as seen in Section 3. □

**Lemma 5.3.** *A fractional ideal $I$ has an integral basis $\{\alpha, \beta\}$ with $\alpha \in \mathbb{Q}^+$ and is characterized by the property as the minimum rational positive in $I$. If $I$ is an integral ideal, then $\alpha \in \mathbb{Z}$.*

*Proof.* Let $\{\alpha, \beta\}$ be an integral basis for the fractional ideal $I$, where $\alpha = a_1 + a_2\sqrt{d}$ and $\beta = b_1 + b_2\sqrt{d}$ with $a_i, b_i \in \mathbb{Q}$. Since we are able to represent any integer $k \in \mathbb{Z}$ with the integral basis, we get that there must exist $m, n \in \mathbb{Z}$ such that $na_2 + mb_2 = 0$, and without loss of generality, suppose $\gcd(m, n) = 1$. Since the $\gcd(m, n) = 1$, there must exist an $x, y \in \mathbb{Z}$ such that $mx - ny = 1$, giving us that the matrix

$$A = \begin{bmatrix} m & n \\ x & y \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

and so we get that

$$A \begin{bmatrix} \alpha & \beta \end{bmatrix} = \begin{bmatrix} m\alpha + n\beta \\ x\alpha + y\beta \end{bmatrix} = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}$$

but due to how we picked out integers $m, n \in \mathbb{Z}$, we get that $\alpha' = m\alpha + n\beta \in \mathbb{Q}$, which we can take to be positive since otherwise we can change the signs on $m, n$ appropriately. Moreover, since the calculation above is a change of integral bases, we get that $\beta' \notin \mathbb{Q}$ since $\alpha, \beta$ are linearly independent over $\mathbb{Q}$. Thus any element of the ideal $x \in I$ must be of the form $x = m\alpha' + n\beta'$ and $x \in \mathbb{Q}$ if and only if $n = 0$, giving us that $\alpha'$ is the smallest positive rational contained in $I$.

Now if $I$ is an integral ideal, then $I \subseteq \mathcal{O}_F = \mathbb{Z}[r]$ where $r = \left(D_F + \sqrt{D_F}\right)/2$. Thus, any element of $\alpha \in I$ will be of the form

$$\alpha = m + n\frac{D_F + \sqrt{D_F}}{2}, \quad \text{where } m, n \in \mathbb{Z}$$

and since $\sqrt{D_F} \notin \mathbb{Q}$, we get that the only rationals in $I$ are precisely the integers. □

Before progressing onto the next theorem, we introduce one piece of notation. Note that for $a, b \in \mathbb{Z}$, that $a\mathbb{Z} + \frac{b}{2}\mathbb{Z} = a\mathbb{Z} + \frac{b'}{2}\mathbb{Z}$ for all $b' \equiv b \bmod 2a$ and so we are able to shift the value of $b$ to be in any specified interval of length $2a$. Let $\tau_{a,b}$ be the unique integer $\tau$ such that $\tau \equiv b \bmod 2a$ such that

$$\begin{cases} -a < \tau \leq a & \text{if } a > \sqrt{D_F} \\ \sqrt{D_F} - 2a < \tau \leq \sqrt{D_F} & \text{else} \end{cases}.$$

Using this notation, we are ready to state how integral ideals are presented:

**Theorem 5.4.** *A subset $I \subseteq F$ is an integral ideal of $\mathcal{O}_F$ if and only if $I$ can be represented in the form*

$$I = ka\mathbb{Z} + k\frac{b + \sqrt{D_F}}{2}\mathbb{Z}$$

*where $a, b, k \in \mathbb{Z}$, where $a, k > 0, b = \tau_{b,a}$ and $4a|(b^2 - D_F)$. Moreover, this representation is unique to the ideal $I$ and $\mathcal{N}(I) = k^2 a$.*

*Proof.* Let $I$ be an integral ideal of $\mathcal{O}_F$. By Lemma 5.3, we can write $I = \alpha\mathbb{Z} + \beta\mathbb{Z}$ with $\alpha \in \mathbb{Z}$ and without loss of generality, suppose $\alpha$ is the least positive integer in $I$ since otherwise we can reduce it via the proof of the previous lemma. Letting $r = \dfrac{D_F + \sqrt{D_F}}{2}$, Thus, it follows that

$$\beta = m_1 + m_2 r = \frac{b' + k\sqrt{D_F}}{2}$$

for some $b', k \in \mathbb{Z}$, where we can assume without loss of generality that $k > 0$ since $\beta\mathbb{Z} = -\beta\mathbb{Z}$. Since $\alpha, r \in \mathcal{O}_F$, we get that for some integers $m, n \in \mathbb{Z}$ that

$$\alpha r = m\alpha + n\beta = m\alpha + n\frac{b' + k\sqrt{D_F}}{2} \Longrightarrow \alpha = nk.$$

That is, $k|\alpha$. Following a similar procedure, since $\dfrac{b' + k\sqrt{D_F}}{2} \in I$, we get there are some integers $n', m' \in \mathbb{Z}$ such that

$$\frac{b' + k\sqrt{D_F}}{2}\frac{D_F + \sqrt{D_F}}{2} = n'\alpha + m'\frac{b' + k\sqrt{D_F}}{2} \Longrightarrow k|b'.$$

Writing $\alpha = ka$ and $b' = kb$, for some $a, b \in \mathbb{Z}$, where $a > 0$, we get that

$$I = \alpha\mathbb{Z} + \frac{b' + k\sqrt{D_F}}{2} = k\left(a\mathbb{Z} + \frac{b + \sqrt{D_F}}{2}\right).$$

These integers are uniquely determined; indeed $ka$ is the least positive coefficient of $\sqrt{D_F}$ due to the same process as the proof in Lemma 5.3, giving us that $a$ is uniquely determined. Moreover, setting $b = \tau_{b,a}$ uniquely determines $b$.

Now since we also have that $k(b+\sqrt{D_F}) \in I$ and $r \in \mathcal{O}_F$, the product gives us

$$\left(k(b+\sqrt{D_F})\right) r = \frac{k(b+1)D_F + (b+D_F)\sqrt{D_F}}{4} \in I$$
$$= kn_1 a + kn_2 \frac{b+\sqrt{D_F}}{2}$$

for some integers $n_1, n_2 \in \mathbb{Z}$. This reveals that $2n_2 = b + D_F$ and that

$$D_F(b+1) = 4an_1 + 2n_2 b = 4an_1 + b^2 + bD_F$$

and so we conclude that $4an_1 = D_F - b^2$.

Conversely, suppose

$$I = k\left(a\mathbb{Z} + \frac{b+\sqrt{D_F}}{2}\mathbb{Z}\right)$$

with the conditions on $a, b, k$ as given above. We will show that $I$ is an (integral) ideal. The set $I$ is clearly closed under addition and multiplication and so it now suffices to check strong multiplication; indeed recall that $\mathcal{O}_F$ has an integral basis given by $\{1, r\}$ and so it suffices to check that $1I \subseteq I$ and $rI \subseteq I$. Since $1I = I$, we now only check for $rI$. Thus, it follows that

$$rI = rk\left(a\mathbb{Z} + \frac{b+\sqrt{D_F}}{2}\mathbb{Z}\right)$$

and we note that $rka\mathbb{Z} \subseteq I$ if and only if

$$rka = ka\left(\frac{D_F+\sqrt{D_F}}{2}\right) = mka + nk\frac{b+\sqrt{D_F}}{2}$$

for some $m, n \in \mathbb{Z}$. Granting the form of the solution, in which case we show that $m, n$ are integers, we get that $ma + (nb)/2 = aD_F/2$ and $n = a$, giving us that $m = (D_F + b)/2$. However, since $b^2 = D_F + 4ac$, we get that $b \equiv D_F \bmod 2$ and so we conclude that $b \equiv D_F \bmod 2$, giving us that $n, m \in \mathbb{Z}$.

Doing the exact same song and dance for $nk(b+\sqrt{D_F})/2$, we calculate that $n = (D_F + b)/2$ which we showed before is an integer and $m = (D_F - b^2)/(4a)$ which is an integer as well due to the assumption on the conditions of $a, b, k$; thus we are done. □

This theorem tells us that the presentation of a principal integral ideal $I$ is given by $(a, b, k) \in \mathbb{Z}^3$ where $ak$ is the minimal positive rational contained in $I$, $k/2$ is the minimal positive coefficient of $\sqrt{D_F}$ among all elements in $I$, and $b = \tau_{b,a}$. That is, specifying the

parameters $a, b, k$ determines the principal ideal $I$ and can be determined in $\text{poly}(\log|x|, \log|y|, \log D_F)$ time.[1]

Since fractional ideals can be viewed as ideals after applying an appropriate scalar multiple of $F$, it follows that a principal fractional ideal $I$ also can be uniquely presented but in the form

$$I = \frac{k}{\ell}\left(a\mathbb{Z} + \frac{b+\sqrt{D_F}}{2}\mathbb{Z}\right)$$

where $\ell \in \mathbb{N}$ is the smallest integer such that $a, b, k$ satisfy the necessary conditions. When $I$ is expressed in this form, we say that $I$ is in *standard form.*

5.2. **Reduced Ideals and Neighbors.** We introduce a geometric picture to help us envision the fractional ideal as a lattice in $\mathbb{R}^2$.

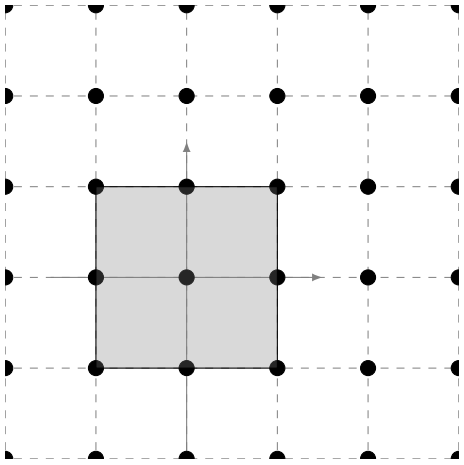


Figure 2

where on the $x$ axis we have $\alpha \in F$ and the $y$ coordinate is given by $\overline{\alpha}$. The corners of the rectangle are $(\pm\alpha, \pm\overline{\alpha})$.

An element $\alpha \in I$ is called a *minimum* if $\alpha > 0$ and there is no nonzero $\beta \in I$ such that $|\beta| < |\alpha|$ and $|\overline{\beta}| < |\overline{\alpha}|$. Pictorially, this only means that there is no lattice point inside the rectangle drawn and $(\alpha, \overline{\alpha})$ is in he right half of the rectangle (see Figure 2). We say that a fractional ideal $I$ is *reduced* if $1 \in I$ and 1 is a minimum in $I$.

[1]This is Proposition 17 in the writeup by [Joz03]; I could not understand why its computation time was precisely this from the writeup.

For any fractional ideal $I$, if $I$ can be written in the form

$$I = \mathbb{Z} + \frac{b + \sqrt{D_F}}{2a}\mathbb{Z},$$

we define $\gamma(I) := \dfrac{b + \sqrt{D_F}}{2a}$ to ease up on notation for the rest of this section.

**Proposition 5.5.** *If $I$ is reduced then its standard form is given by*

$$I = \mathbb{Z} + \gamma(I)\mathbb{Z}$$

*where $(a, b, k, \ell)$ are the parameters as before, i.e., we have $k = 1$ and $\ell = a$.*

*Proof.* If $I$ is reduced, then there exists integers $m, n \in \mathbb{Z}$ such that

$$1 = \frac{k}{\ell}(na + mb + m\sqrt{D_F}).$$

From this, we see that $m = 0$ and $kna/\ell = 1$. Without loss of generality, we can take $n > 0$. Supposing $n > 1$, then it follows that $ka(n-1)/\ell < 1$ from the equality above and moreover, we have that this is a point in $I$, contradicting minimality of 1. Thus $n = 1$ and so we get that $ka/\ell = 1$, and by the minimality assumption on $\ell$, we get that $k = 1$. □

**Proposition 5.6.** *Let $I$ be a reduced ideal in standard form, given by the parameters $(a, b, k, \ell)$. Then $a < \sqrt{D_F}$ and $|b| < \sqrt{D_F}$ as well. Thus, we conclude that there are a finite number of reduced ideals.*

*Proof.* Suppose that $a > \sqrt{D_F}$. Recalling the definition of $\tau_{b,a}$, it follows that $\tau_{b,a}$ is the integer $\tau$ such that $\tau \equiv b \bmod 2a$ such that $|\tau| < a$. Taking $b = \tau_{b,a}$, we have that $|b| < a$ and so it follows that $b + \sqrt{D_F} < 2a$ and so

$$\left|\frac{b + \sqrt{D_F}}{2a}\right| < 1 \quad \text{and} \quad \left|\frac{b - \sqrt{D_F}}{2a}\right| < 1$$

and since $(b + \sqrt{D_F})/(2a) \in I$, we have a contradiction on the minimality of 1. Thus $a < \sqrt{D_F}$ and by the definition of $\tau_{b,a}$, we get that $|b| < \sqrt{D_F}$. □

We now characterize reduced forms:

**Proposition 5.7.** *If $I$ is a fractional ideal with standard form given by*

$$I = \mathbb{Z} + \gamma(I)\mathbb{Z},$$

*$I$ is reduced if and only if $b \geq 0$ and $b + \sqrt{D_F} > 2a$.*

*Proof.* Suppose $I$ is reduced. By the previous proposition, we have that $a < \sqrt{D_F}$ and so $b = \tau_{b,a}$ is an integer living between $\sqrt{D_F} - 2a < b < \sqrt{D_F}$. If $b < 0$, then $-b < 2a - \sqrt{D_F}$

giving us that $-b+\sqrt{D_F} < 2a$ and thus

$$\left|\frac{b \pm \sqrt{D_F}}{2a}\right| \leq \frac{|b|+\sqrt{D_F}}{2a} < 1,$$

contradicting minimality of 1. Thus, we conclude that $b \geq 0$. To show that $b+\sqrt{D_F} > 2a$, suppose the opposite is true and using the same exact argument, we arrive at a contradiction since $(b+\sqrt{D_F})/(2a) < 1$ will be a contradiction to the minimality of 1.

Conversely, suppose $b \geq 0$ with $b+\sqrt{D_F} > 2a$. Defining a function

$$H(x,y) = \max\left\{|2xa + y(b \pm \sqrt{D_F})|\right\}$$

we see that through calculations that 1 is a minimum of $I$ if and only if $H(x,y) > 2a$ for all $(x,y) \in \mathbb{Z}^2 - \{(0,0)\}$. However, since $H$ has the property that $H(-x,-y) = H(x,y)$, it suffices to consider the cases where $x, y \geq 0$ and $x > 0, y \leq 0$.

For the first case, where $x, y \geq 0$, both not zero simultaneously, we get that

$$b+\sqrt{D_F} > 2a \Longrightarrow |2xa + y(b+\sqrt{D_F})| \geq 2xa + 2ya \geq 2a.$$

For the second case, where $x > 0$ and $y \leq 0$, it follows that

$$b+\sqrt{D_F} > 2a \Longrightarrow \sqrt{D_F} + (b-a) > a.$$

Now if $a > \sqrt{D_F}$, then $b = \tau_{b,a}$ gives us that $b < a$ and therefore a contradiction. Thus $a < \sqrt{D_F}$ and so we so using $b = \tau_{b,a}$ gives us that $b < \sqrt{D_F}$ and $b - \sqrt{D_F} < 0$. Therefore, we get that

$$|2xa - y(b-\sqrt{D_F})| = 2xa + |y(b-\sqrt{D_F})| > 2xa$$

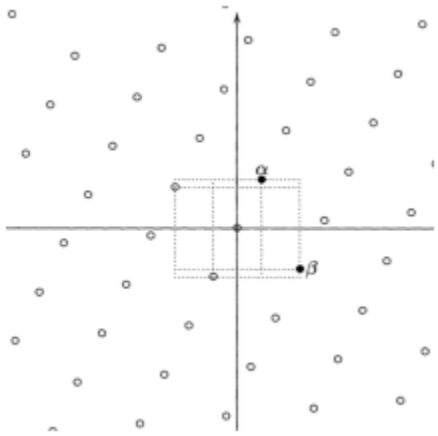
but since $x > 0$, we conclude that $H(x,y) \geq 2a$. □

From this characterization, we get the following corollary:

**Corollary 5.8.** *A fractional ideal $I = \mathbb{Z} + \gamma(I)\mathbb{Z}$ is reduced if $a \leq \sqrt{D_F}/2$.*

*Proof.* Let $I = \mathbb{Z} + \gamma(I)\mathbb{Z}$. If $a \leq \sqrt{D_F}/2$, we get that $b = \tau_{b,a} > 0$ and thus $b+\sqrt{D_F} \geq b + 2a > 2a$ giving us that $I$ is reduced. □

Let $I$ is a fractional ideal of $\mathcal{O}_F$ and let $\alpha \in I$ be a minimum. We define the *right neighbor* of $\alpha$ to be the uniquely determined smallest minimum $\beta_R \in I$ such that $\beta_R > \alpha$ and we define the *left neighbor* of $\alpha$ to be the uniquely determined smallest minimum $\beta_L \in I$ such that $|\overline{\beta_L}| > |\overline{\alpha}|$. We can picture this geometrically as shown in the figure below in [BvdP10], page 170.




**Proposition 5.9.** *Let $\alpha \in F$ with $\alpha > 0$. Then the map $I \to \alpha I$ sending $x \longmapsto \alpha x$ is a bijection mapping minima to minima, left neighbors to left neighbors, and right neighbors to right neighbors for any fractional ideal $I$.*

*Proof (Sketch).* Since $\alpha \in F$, we get that this is a bijection. To see why minima get taken to minima, and neighbors get taken to respective neighbors, we scale all lattice points by $\alpha$ and $\overline{\alpha}$ in the $x$ and $y$ directions respectively, sending all of the minima to minima in the image and neighbors to neighbors. □

**Proposition 5.10.** *If $I = \mathbb{Z} + \gamma(I)\mathbb{Z}$ is a reduced, then $\gamma(I) > 1$ and $-1 < \overline{\gamma(I)} < 0$.*

*Proof.* For a reduced ideal $I$, we see that $\gamma(I) = (b + \sqrt{D_F})/(2a) > 1$ by the characterization of reduced ideals. Thus, we have that $a < \sqrt{D_F}$ and $\sqrt{D_F} - 2a < b \leq a < \sqrt{D_F}$ and so we get bounds

$$-1 < \frac{b - \sqrt{D_F}}{2a} = \overline{\gamma(I)} < 0.$$

□

For ideals that can be written in the form $\mathbb{Z} + \gamma(I)\mathbb{Z}$, we introduce the *reduction operator* $\rho : \mathcal{P}(F) \to \mathcal{P}(F)$ defined by

$$\rho(I) = \frac{1}{\gamma(I)} I + \frac{2a}{b + \sqrt{D_F}}\mathbb{Z} + \mathbb{Z}.$$

Recalling that $4a|(b^2 - D_F)$, let $c = |D_F - b^2|/(4a)$ and so it follows that

$$\begin{aligned} \frac{2a}{b + \sqrt{D_F}}\mathbb{Z} + \mathbb{Z} &= \frac{2a(b - \sqrt{D_F})}{b^2 - D_F}\mathbb{Z} + \mathbb{Z} \\ &= \frac{-b + \sqrt{D_F}}{2c}\mathbb{Z} + \mathbb{Z} \end{aligned}$$

$$= \frac{\tau_{-b,c} + \sqrt{D_F}}{2c}\mathbb{Z} + \mathbb{Z}$$

where the final equality shows that this is in standard form, i.e. the parameters for $\rho(I)$ are precisely $(a', b', k, \ell) = (c, \tau_{-b,c}, k, \ell)$.

**Theorem 5.11.** *Let $I = \mathbb{Z} + \gamma\mathbb{Z}$ be a fractional ideal. Letting $I_0 = I$ and for all $i \in \mathbb{Z}$, define*

$$I_i := \rho(I_{i-1}) = \mathbb{Z} + \gamma_i\mathbb{Z}, \quad \gamma_i = \frac{b_i + \sqrt{D_F}}{2a_i}.$$

*If $I_i$ is not reduced, then $a_i < a_{i-1}/2$, and so $I_i$ is reduced for some $i \leq \lceil \log_2(a/\sqrt{D_F})\rceil + 1$. Letting $i_{\min}$ be the minimal among all $i$ such that $I_i$ is reduced, defining $\alpha := \prod_{j=1}^{i_{\min}-1}\gamma_j$, we get that $\alpha$ is a minimum in $I$ and moreover, $I_{red} = \frac{1}{\alpha}I$.*

*Proof.* Suppose $I_i$ is reduced, giving us that $b_i + \sqrt{D_F} > 2a_i$. Without loss of generality, we can take that $a_{i+1} < \sqrt{D_F}$ since if we took $a_{i+1} > \sqrt{D_F}$, then by the $b = \tau_{b,a}$ definition, we get $|b_{i+1}| < a_{i+1}$ and combining the inequalities above gives us

$$a_{i+1} \leq \frac{|b_i^2 - D_F|}{4a_i} < \frac{a_i^2 + D_F}{4a_i} < \frac{a_i}{2}.$$

We now consider the two cases where we either have $a_{i+1} \geq a_i$ or $a_{i+1} < a_i$.

In the first case, since we have the (additional) inequalities $\sqrt{D_F} - 2a_i < b_i < \sqrt{D_F}$, we get that $D_F - b_i^2 \geq 4a_i^2$. Thus, we conclude that $\sqrt{D_F} + |b_i| > 2a_i$. Now to show that we have that $I_i$ is reduced, we need that $b_i \geq 0$. Suppose not. Then it follows that

$$\sqrt{D_F} - 2a_i < b_i < 0 \Longrightarrow |b_i| < 2a_i - \sqrt{D_F}$$

giving us a contradiction.

In the second case, if $a_{i+1} < a_i$, then $a_{i+1}^2 < a_i a_{i+1} \leq a_i r(b_i - \sqrt{D_F}) = (D_F - b_i^2)/4$ and so we get that $a_{i+1} < \sqrt{D_F}/2$, and thus $I_{i+1}$ is reduced.

It is clear that $I_{red} = \frac{1}{\alpha}I$, and since this is reduced, we get that $\alpha$ must be a minimum. □

**Proposition 5.12.** *If $I = \mathbb{Z} + \gamma(I)\mathbb{Z}$ is reduced, then*

*(1) $\gamma(I)$ is a minimum*
*(2) $\rho(I)$ is reduced.*

*Proof.* We first show that $\gamma = \gamma(I)$ is a minimum. Let $x + y\gamma \in I$ such that $|x + y\gamma| < |\gamma|$ and $|x + y\overline{\gamma}| \leq |\overline{\gamma}|$. Without loss of generality, suppose $x \geq 0$. It follows that $\gamma > 1$ and since $|x + \gamma y| < |\gamma|$, we can compute that $y \leq 0$.

Now if $|x + y\overline{\gamma}| < |\overline{\gamma}|$, we get that

$$-|\overline{\gamma}| < |x - y|\overline{\gamma}| \, | < |\overline{\gamma}|$$

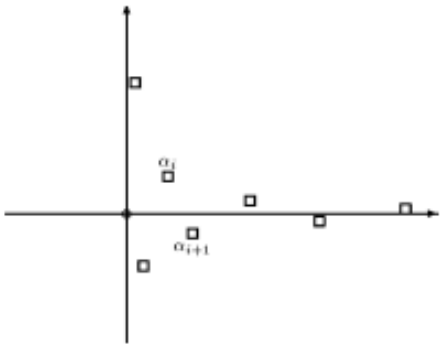
and it is clear that since $x \geq 0$ that $-y|\overline{\gamma}| < |\overline{\gamma}|$, giving us that $y > -1$ and so we conclude that $y = 0$. Since $|\overline{\gamma}| < 1$, but we have that $|x| < |\overline{\gamma}| < 1$, we conclude that $x = 0$ as well. Thus, we conclude that $\gamma$ is a minimum, and by the bijection , we get that $\rho(I)$ is reduced as well. □

5.3. **Principal Cycles.** Recalling Proposition 5.7, we note that the ring of integers $\mathcal{O}_F = \mathbb{Z} + \dfrac{D_F + \sqrt{D_F}}{2}$ is a reduced principal ideal of itself, giving us that $1 \in \mathcal{O}_F$ is a minimum. For $i \in \mathbb{Z}$, set $\alpha_{i+1}$ to be the right neighbor of $\alpha_i$ and $\mathfrak{J}_i = \mathcal{O}_F/\alpha_i$. Since each $\alpha_i \in \mathcal{O}_F$ are minimums, we get by the bijection that $1 \in \mathfrak{J}_i$ is a minimum, giving us that $\mathfrak{J}_i$ is reduced. Defining

$$\gamma_i = \frac{b_+\sqrt{D_F}}{2a_i},$$

we get that since $I_i$ is reduced, it is of the form $I_i = \mathbb{Z} + \gamma_i\mathbb{Z}$ for some $a_i, b_i$. Furthermore, by Proposition 5.12, we get that $\alpha_{i+1}/\alpha_i = \gamma_i$.

Geometrically, we can envision it as a pair of hyperbolas that alternate signs (picture from [BTW95]).




**Lemma 5.13.** *For all $i \in \mathbb{Z}$, we have that $\ln \alpha_{i+1} - \ln \alpha_i \leq \ln \sqrt{D_F}$.*

*Proof.* Since each $I_i$ is reduced, we can use Proposition 5.6 to give us bounds $|b_i| \leq \sqrt{D_F}$. Thus, we have that

$$\gamma_i = \frac{b_i + \sqrt{D_F}}{2a_i} \leq \frac{2\sqrt{D_F}}{2a_i} \leq \sqrt{D_F}$$

and since ln is a strictly increasing we are done. □

While this gives us an upper bound on the differences, we also have a lower bound:

**Lemma 5.14.** *For all $i \in \mathbb{Z}$, we have that* $\ln \alpha_{i+1} - \ln \alpha_{i-1} > \ln 2$.

*Proof.* As we see, the $\overline{\alpha_{i-1}}$ and $\overline{\alpha_{i+1}}$ share the same sign and and since the $|\overline{\alpha}_i|$ forms a strictly decreasing sequence, we get that

$$|\overline{\alpha}_{i+1} - \overline{\alpha}_{i-1}| < |\overline{\alpha}_{i-1}|$$

If we have that $\alpha_{i+1}/\alpha_{i-1} < 2$, then we have

$$\alpha_{i-1} < \alpha_{i+1} < 2\alpha_{i-1}$$

and so $0 < \alpha_{i+1} - \alpha_{i-1} < \alpha_{i-1}$. This contradicts the minimality assumption of $\alpha_{i-1}$. □

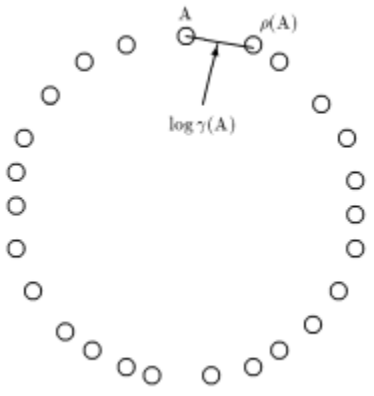
**Theorem 5.15.** *(1) The sequence $\{\mathfrak{J}_i\}_{i\in\mathbb{Z}}$ is periodic, i.e., there exists a $k \in \mathbb{N}$ such that $\mathfrak{J}_i = \mathfrak{J}_j$ if and only if $i \equiv j \bmod k$ for all $i, j \in \mathbb{Z}$. This forms a cycle and the length of the sequence is called the* period length *and the principal reduced ideals in the period length are called the* **principal cycle**.

*(2) Let $u = \alpha_k/\alpha_0$. We get that $u$ is a unit of $\mathcal{O}_F$ and moreover, it is the fundamental unit.*

*(3) Any reduced principal fractional ideal is contained in the principal cycle.*

*Proof.* We omit the proof and instead direct the reader to [BTW95], Theorem 2.30. □

A picture of the cycle is given by [BTW95] where $A$ is the principal reduced ideal $\mathcal{O}_F$.




**Lemma 5.16.** *For any $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, we have that*

$$\lfloor n/2 \rfloor \ln(2) \leq \ln \alpha_{m+n} - \ln \alpha_m \leq n \log \sqrt{D_F}.$$

*Proof.* Expressing $\ln \alpha_{m+n} - \ln \alpha_m$ as a telescoping sum,

$$\ln \alpha_{m+n} - \ln \alpha_{m+(n-1)} + \ln \alpha_{m+(n-1)} - \cdots + \ln \alpha_{m+1} - \ln \alpha_m$$

and applying the Lemma 5.13 and Lemma 5.14 immediately gives us our desired result. □

**Lemma 5.17.** *If $k$ denotes the period length of the principal cycle, then*

$$\frac{2R}{\ln D_F} \leq k \leq \frac{2R}{\ln 2}.$$

*Proof.* Since $R = \ln u_0 = \ln \alpha_k - \ln \alpha_0$, where $\alpha_0 = 1$, the lower bound of the previous lemma tells us that $(k/2) \ln 2 \leq R$ and thus $k \leq 2R/\ln(2)$. Similarly, the upper bound of the previous lemma gives us that $k \ln D \geq 2R$. □

Let $I = \mathbb{Z} + \gamma(I)\mathbb{Z} = \mathbb{Z} + \frac{b+\sqrt{D_F}}{2a}\mathbb{Z}$. Since $a > 0$ can be arbitrarily large, there are infinitely many ideals of this form but at the same time, recall that we can apply the reduction operator $\rho$ sufficiently many times on $I$ to obtain a reduced ideal. Since $\mathcal{P}_F$ only has finitely many reduced ideals, we get that the reduction operator cannot be injective; however, we can restrict our focus to strictly reduced principal ideals, i.e., the ideals within the principal cycle. Denoting $\mathcal{P}_r(F)$ to denote the principal cycle, i.e.,

$$\mathcal{P}_r(F) = \{\mathfrak{J}_0 = \mathcal{O}_F, \mathfrak{J}_1, \ldots, \mathfrak{J}_{k-1}\}$$

where $\mathfrak{J}d_{i+1}$ is the right neighbor of $\mathfrak{J}_i$, i.e., $\mathfrak{J}_{i+1} = \rho(\mathfrak{J}_i)$ for all $i \in \mathbb{Z}/k\mathbb{Z}$. It becomes intuitive that we may want to define the inverse reduction operator gives the left neighbor of a minimum.

Now to actually go about this, define the conjugated ideal of $I$ to be

$$\overline{I} = \mathbb{Z} + \frac{b - \sqrt{D_F}}{2a}\mathbb{Z} = \mathbb{Z} + \frac{\tau_{-b,a} + \sqrt{D_F}}{2a}\mathbb{Z}.$$

Clearly, if $I$ is reduced, then $\overline{I}$ is also reduced since 1 is invariant under conjugation.

Geometrically, we can envision the conjugated ideal to be a reflection of the lattice, given by $I$, across the $y = x$ line; this gives us intuition that if $\alpha$ is a minimum in $I$, then $|\overline{\alpha}|$ is a minimum in $\overline{I}$. Moreover, this also fits the idea that the inverse reduction operator gives the left neighbor of a minimum. Now more concretely, we define the inverse reduction operator to be

$$\rho^{-1} = \frac{2a}{\sqrt{D_F} - \tau_{-b,a}} \left( \mathbb{Z} + \frac{b + \sqrt{D_F}}{2a}\mathbb{Z} \right).$$

## 6. The Ideal Distance (CDC says 6 feet)

If $I$ and $J$ are fractional principal ideals of $\mathcal{O}$ and there exists an $\alpha \in F$ such that $I = \alpha J$, we define the *distance* between $I$ and $J$ to be

$$\delta(I, J) = \ln |\alpha| \bmod R, \quad R = \ln(u_0)$$

where $R$ is the regulator and $u_0$ is the fundamental unit of $F$. If there is no such $\alpha \in F$ relating the two fractional ideals, we say that the distance is not defined. We first check that the distance, when defined, is actually well defined since there may multiple elements relating $I$ and $J$. Thus, suppose we have $\alpha, \beta \in F$ such that $I = \alpha J$ and $I = \beta J$. That is, we have that

$$\alpha J = I = \beta J$$

and since these are principal ideals, by Proposition 4.1, we get that $\alpha = \beta u = \beta u_0^r$ where $u$ was just some unit and $r \in \mathbb{Z}$. Thus, we get that $\ln |\alpha| = \ln |\beta u_0^k| = \ln |\beta| + kR$, and so we see that the distance is well defined. From the definition of the distance, it is easy to compute that $\delta(I, J) = -\delta(J, I)$

We will be studying primarily the distance $\delta(\mathcal{O}_F, I)$ for a principal fractional ideal $I$. Abusing notation, we will denote this distance as $\delta(I)$.

### 6.1. **Jumping.**

As we will be interested in the case of $I^n$ for possibly very large $n$ from $I$, we want to be able to speed up the process. Just as in modular exponentiation, we study iterations of squares but before being able to make such jumps, we should be able to convert a product of ideals into standard form in terms of the standard forms of the productands.

**Proposition 6.1.** *Let*

$$I_i = a_i\mathbb{Z} + \gamma_i\mathbb{Z}, i = 1, 2$$

*be principal ideals. There exists a standard presentation for the product $I_1 I_2$.*

*Proof.* We omit the proof as this writeup is already getting quite long. See [Joz03], Proposition 34 for details. □

It should be noted that even if $I$ and $J$ are reduced that the product $IJ$ itself is not necessarily reduced. Moreover, from this definition of products, it is clear that $\delta(IJ) \equiv \delta(I) + \delta(J) \bmod R$.

Now specializing to the case that $I = J$, where $I$ is a reduced ideal in the principal cycle,

$$I = \mathbb{Z} + \gamma(I)\mathbb{Z} = \frac{1}{a}\left(a\mathbb{Z} + \frac{b + \sqrt{D_F}}{2}\mathbb{Z}\right).$$

Thus, if we consider $I^2$, we can rewrite it into standard form as

$$I^2 = I \cdot I = \frac{k'}{a'}\left(a'\mathbb{Z} + \frac{b'\sqrt{D_F}}{2}\mathbb{Z}\right)$$

where for some $a', b', k' \in \mathbb{Z}$, which are computable by the proof of Proposition 6.1. Thus, with these values, we have that

$$I^2 = \frac{1}{k'}\left(\mathbb{Z} + \frac{b' + \sqrt{D_F}}{2a'}\right).$$

Since the triple $(a', b', k')$ form a standard triple for parameters of an ideal, consider the ideal parametrized by this triple:

$$I_2' = \mathbb{Z} + \frac{b' + \sqrt{D_F}}{2a'}\mathbb{Z}.$$

Since $I$ is assumed to be reduced, we get that $0 < a, b < \sqrt{D_F}$ and so $k' = \gcd(a, b) < \sqrt{D_F}$ as well. Computing that $|\delta(I_2, I_2')| = \ln k' < \ln \sqrt{D_F}$, apply the reduction operator on $I_2'$ to get that $(I_2')_{\text{red}}$ which is in the principal cycle.

Denote $I^{(2)} = I * I$ to be the first principal reduced fractional ideal $\mathfrak{J}_i$ for some $i$.

We now estimate the computational complexity of computing $I^{(2)}$. Since $I$ is reduced, we have that both $a, b = O(\sqrt{D_F})$ and so $k = \gcd(a, b) = ua + vb$ for some $u, v \in \mathbb{Z}$. Making the substitutions

$$u \longmapsto u - xb, \quad w \longmapsto w + xa, \quad x \in \mathbb{Z}$$

gives us that we can always find a $u \in \mathbb{Z}$ such that $u < b = O(\sqrt{D_F})$ and similarly, we get that $w = O(\sqrt{D_F})$ giving us that $k' = O(D_F)$. Thus, we are able to compute all of the $a', b', k'$ in $O(D_F^2)$ in the worst case scenario, with arithmetic operations being completed in $O(\text{poly} \log D_F)$ time.

Since the reduction operator requires $O(\log(a'/\sqrt{D_F})$, where $a' = O(D_F^2)$, applying the square of the reduction operator at most $O(\ln D_F)$ times (see discussion above), we conclude that the computation of $I * I$ is $O(\text{poly} \log D_F)$.

This proves the following:

**Proposition 6.2.** *Let $I$ be a reduced principal fractional ideal. Consider iterations of squares of $I$, i.e.,*

$$I \longmapsto I^{(2)} = I * I \longmapsto I^{(4)} = I^2 * I^2 \longmapsto \cdots \longmapsto I^{(2^n)} = I^{(2^{n-1})} \cdot I^{(2^{n-1})}.$$

*We have that $\delta(I^{2^n}) > 2^n\delta(I)$ before reducing the distances modulo $R$. The distance of the ideal, before reduction modulo $R$, can be computed in $O(\text{poly}(\log(D), n)$ time.*

## 7. Hallgren's Algorithm

Let $\mathcal{P}_r$ denote the set of all reduced principal fractional ideals and define the following function $h : \mathbb{R} \longrightarrow \mathcal{P}_r \times \mathbb{R}$ as follows: Let $\widetilde{x}$ be a fixed real number such that $0 \leq \widetilde{x} < R$. Then, for any $x \equiv \widetilde{x} \bmod R$,

$$h(x) = (I_x, \widetilde{x} - \delta(I_x))$$

where $I_x \in \mathcal{P}_r$ is the ideal with the greatest distance such that $\delta(I_x) < \widetilde{x}$. It is clear from this definition that $h$ is periodic and also one to one on the quotient $\mathbb{R}/R$.

With this function, and our entire story of ideals, we come to the following result:

**Theorem 7.1.** *The function $h$ is computable in polynomial time. If $x$ is an integer multiple of $10^-n$, we can compute the reduced principal fractional ideal $I_x$ precisely and approximate $\widetilde{x} - \delta(I_x)$ in $\text{poly}(\log(D_F), \log x, n)$ time, accurate to $10^{-n}$.*

*Proof.* Recall that the reduction operator on a reduced ideal can be computed in $\text{poly}(\log(D_F))$ time. Noting that $\mathcal{O}_F$ can be parametrized by $(\tau_{D_F,2}, 1)$ with $\delta(\mathcal{O}_F) = 0$,

Let $I_0 := \rho^2(\mathcal{O}_F)$ with $\ln D_F > \delta(I_0) > \ln 2$. Using the iterated $*$-squaring to construct a sequence of ideals, where $I_{i+1} = I_i * I_i$, it follows that

$$2\delta(I_{i-1}) \leq \delta(I_i) \leq 2\delta(I_{i-1}) + \ln\sqrt{D_F}$$

and so we get that $2^k\delta(I_0) \leq \delta(I_i)$; terminate the sequence for $i = N$ where $N$ is the integer such that $\delta(I_{N+1})$ first exceeds $x$, which is guaranteed to happen for $N < \lceil \log_2(x/A) \rceil$.

Next, once we are at a reduced ideal $\mathfrak{J}$, and are using $I_i$, compute $\mathfrak{J} * I_i$ with

$$\delta(\mathfrak{J}) + \delta(I_k) \leq \delta(\mathfrak{J} * I) \leq \delta(\mathfrak{J}) + \delta(I) + \ln\sqrt{D_F}.$$

After this, make the change $\mathfrak{J} \longmapsto \mathfrak{J} * I_i$ as long as $\delta(\mathfrak{J} * I_i) < x$. If we exceed $x$, then take try $\mathfrak{J} * I_{i-1}$. After $O(\log x)$ steps, we will have computed a reduced ideal $\mathfrak{J}_r$ that is to the left of $x$ with the bounds

$$x = \delta(\mathfrak{J}_r) \leq A + \ln\sqrt{D_F} \leq \frac{3}{2}\ln D_F.$$

While running this algorithm, run computations to evaluate $\delta(I, \rho(I))$ for $I = \mathbb{Z} + \gamma(I)\mathbb{Z}$, which by the previous proposition, will give us our desired accuracy.

Now applying the reduction operator on the reduced ideal $\mathfrak{J}_r$ until its distance is greater than $x$, which will require at most $(3/2)\ln(D_F)/\ln(2)$ steps, we get an ideal $\mathfrak{J}'$ which will be the last such ideal that is to the left of $x$. Then we get that $I_x = \mathfrak{J}'$ or its reduction $\rho(\mathfrak{J}')$. Since arithmetic operations of $n$-digits is computable in $\text{poly}(n)$ time, this entire process gives the value of $h(x)$ in $\text{poly}(\log D_F, \log x, n)$ time. □

7.1. **The Quantum Algorithm.** Let $R$ be a real number and suppose we have a function $f : \mathbb{R} \longrightarrow X$ be periodic for some space $X$. We will be applying the quantum period finding algorithm and to do so, we must be able to break $f$, and $X$ if necessary, into discrete values. This leads us to only consider certain types of periodic functions, namely *weakly periodic functions*. A function $f : \mathbb{Z} \to X$ is *weakly periodic* with period $S \in \mathbb{R}$ if for all $0 \leq k \leq \lfloor S \rfloor$ and $m \in \mathbb{Z}$, either

$$f(k + \lfloor mS \rfloor) = f(k) \quad \text{ or we have } f(k + \lceil mS \rceil) = f(k).$$

For convenience, we will simply be writing $[mS]$ to denote the appropriate integer.

Thus, we can discretize the function $h$ with period $R$, as defined as the beginning of the section, by sending $x$ to its nearest multiple of $1/N$, i.e., we have

$$\begin{aligned} h &: \mathbb{R} \longrightarrow \mathcal{P}_r \times \mathbb{R} & h(x) &= ((I_x, \widetilde{x} - \delta(x)) \\ \widetilde{h}_N &: \mathbb{Z} \longrightarrow \mathcal{P}_r \times \frac{1}{N}\mathbb{Z} & \widetilde{h}_N(k) &= (I_{k/N}, \lfloor k/N - \delta(I_{k/N}) \rfloor_N). \end{aligned}$$

Using the notation above,

**Proposition 7.2.** *(1) $\widetilde{h}_N$ is injective on $0 \leq k \leq \lfloor NR \rfloor$*

*(2) $\widetilde{h}_N(x)$ is computable in $\text{poly}(\log x, \log N, \log d)$ time and so if $N$ and $x$ are $O(\text{poly}(d))$, then $\widetilde{h}_N(x)$ is computable in poly$(\log d)$ time.*

*(3) Letting $d_m$ be the lower bound on the minimum distance between reduced ideals, let $\sigma = \log d$ be the input size for the computation. If $N$ is sufficiently large, then $\widetilde{h}_N$ is weakly periodic with period $NR$.*

*Proof.* We omit the proof. For details, see [Joz03], proof of Proposition 36. □

We state the following two lemmas without proof. For details, see [Joz03], page 28.

**Lemma 7.3.** *If $q > 3S^2$, where $q$ is a power of 2, and if $c = [\frac{kq}{S}], d = [\frac{\ell q}{S}]$ with $\gcd(k, \ell) = 1$, then*

$$\left| \frac{c}{d} - \frac{k}{\ell} \right| < \frac{1}{2\ell^2}.$$

**Lemma 7.4.** *Let $|A| \leq 1/2$, and let $\xi(j)$ be a function such that $|\xi(j)| < 1/n$ with $n = O(\log p)$. Then there exists a constant $c$ such that for all sufficiently large $p$,*

$$\left| \sum_{j=0}^{p-1} e^{2\pi i(\frac{A}{p}j + \xi(j))} \right|^2 \geq cp^2.$$

These lemmas help prove the following theorem:

**Theorem 7.5.** *Let $f : \mathbb{Z} \longrightarrow X$ be a wearkly periodic function with period $S$ and suppose the following conditions hold:*

*(1) $f(k)$ is computable in $\text{poly}(\log k, \log S)$ time;*
*(2) $f$ is injective for all $0 \leq k \leq \lfloor S \rfloor$;*
*(3) there exists a $\text{poly}(\log(S))$ time algorithm that will test whether or not any $n \in \mathbb{Z}$ is close to an integer multiple of $S$, i.e., test $|jS - n| < 1$;*

*Then there exists a quantum algorithm that outpus an integer $a$ with $|S - a| < 1$ in $\text{poly}(\log S)$ time with probability at least $1/\text{poly}(\log(S))$.*

*Proof (Sketch).* [2] Given the weakly periodic function $f$, by the first assumption, we can construct the state

$$|\psi_0\rangle \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} |m\rangle \left|f(m)\right\rangle, \quad q = 2^N, N \in \mathbb{N}, q > 3S^2$$

in $\text{poly}(\log(S))$ time. Writing $q = pS + r$ (the first step in the Euclidean algorithm), we note that since $f$ is weakly periodic that we get a superposition over all points $w \equiv k \bmod S$, where $0 \leq k \leq \lfloor S \rfloor$ which is chosen uniformly. Performing a measurement on the second register and discarding it, all while leaving the first register alone, we are left with the state

$$|\psi_1\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \left|k + [jS]\right\rangle.$$

Applying quantum Fourier transform over $\mathbb{Z}/q\mathbb{Z}$ to $|\psi_1\rangle$ gives us

$$\frac{1}{\sqrt{pq}} \sum_{j=0}^{p-1} \sum_{m=0}^{q-1} e^{\frac{2\pi i m}{q}(k+[jS]} |m\rangle = \frac{1}{\sqrt{pq}} \sum_{m=0}^{q-1} e^{2\pi i m k/q} \sum_{j=0}^{p-1} e^{(2\pi i m[jS])/q} |m\rangle.$$

Writing $[jS] = jS + \delta_j$ where $-1 < \delta_j < 1$, also consider $m \in \mathbb{Z}/q\mathbb{Z}$ that are close a integer multiple of $q/S$ that are not too large, i.e.,

$$m = \left[\frac{kq}{S}\right] = \frac{kq}{S} + \varepsilon, \quad m < \frac{q}{\log S},$$

[2] I honestly couldn't follow the final part of the proof for this Theorem (see Theorem 6 in [Joz03] once continued fractions were introduced). The "proof" outlined here is my guess on how the proof is supposed to go, up to the point where I couldn't follow any longer.

where $0 \leq k \leq S$ and $|\varepsilon| \leq 1/2$. It follows form this that

$$\frac{m[jS]}{q} = \left(\frac{k}{S} + \frac{\varepsilon}{q}\right)\left(jS + \delta_j\right) = kj + \frac{k}{S}\delta_j + \frac{\varepsilon jS}{q} + \frac{\varepsilon\delta_j}{q}.$$

Thus, we get that since the Fourier transform is $\mathbb{Z}$-periodic that

$$\frac{1}{\sqrt{pq}}\sum_{m=0}^{q-1} e^{2\pi imk/q}\sum_{j=0}^{p-1} e^{(2\pi im[jS])/q}\,|m\rangle = \frac{1}{\sqrt{pq}}\sum_{m=0}^{q-1} e^{2\pi imk/q}\sum_{j=0}^{p-1} e^{2\pi i(\xi(j)+A/p)}\,|m\rangle$$

where $\xi(j) = \dfrac{k\delta_j}{S} + \dfrac{\varepsilon\delta_j}{q}$ and $A = (\varepsilon jSp)/(q)$.

Denote

$$a_m = \frac{1}{\sqrt{pq}}\sum_{j=0}^{p-1} e^{2\pi i(\xi(j)+A/p)}.$$

Now since we have the bounds on $m < q/(\log(S))$ and $|\varepsilon| \leq (1/2)$, it follows that

$$\frac{m}{q} = \frac{k}{S} + \frac{\varepsilon}{q} < \frac{1}{\log S} + \frac{1}{2q}$$

and since $q > 3S^2$,

$$|\xi(j)| = \left|\frac{k\delta_j}{S} + \frac{\varepsilon\delta_j}{q}\right| < \frac{1}{\log S} + \frac{1}{2q} + \frac{1}{2q} \leq \frac{2}{\log S}.$$

Now, since $|A| \leq |\varepsilon| \leq 1/2$, we can use the previous lemma to give us a constant $c$ such that

$$|a_m| \geq \frac{1}{pq}cp^2 \geq \frac{cp}{pS} = \frac{c}{S}$$

and so for each $m$ that we consider, we have $prob(m) \geq c/S$.Since $m \leq q/\log(S)$, we get that the probability of getting an $m$ that we want to consider is at least $c/\log(S)$.

Repeating this process twice gives two values $j$ values. Calling the two values $c, d$ respectively, we get that

$$c = [\frac{kq}{S}], \quad d = [\frac{\ell q}{S}]$$

with $\gcd(k, \ell) = 1$ with probability $1/\text{poly}(\log S)$.

Through the use of continued fractions, and their convergence, we eventually output a value $n$ such that $|S - n| < 1$ with probability $1/\text{poly}(\log S)$. □

In light of this result, and the use of Proposition 7.2, we are led to the following result:

**Theorem 7.6.** *If $d \in \mathbb{N}$ is square free, there is a quantum algorithm that will output the regulator of $\mathbb{Q}(\sqrt{d})$ to the accuracy of $10^{-n}$, with run time $\text{poly}(\log d, n)$, and with success probability $1/(\text{poly}(\log d, n))$ as long as $10^{-n}$ is sufficiently small.*

## References

[BTW95] Johannes A. Buchmann, Christoph Thiel, and Hugh C. Williams, *Short representation of quadratic integers*, 1995.

[BvdP10] W. Bosma and A. van der Poorten, *Computational algebra and number theory*, Mathematics and Its Applications, Springer Netherlands, 2010.

[DS06] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, Springer New York, 2006.

[IR13] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, Springer New York, 2013.

[Joz03] Richard Jozsa, *Notes on hallgren's efficient quantum algorithm for solving pell's equation*, 2003.