Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 48(1), 2021, Pages 53–62
ISSN: 1223-6934

On the key-exchange protocol using real quadratic fields

Abdelmalek Azizi, Jamal Benamara, Moulay Chrif Ismaili,
and Mohammed Talbi

Abstract. To prevent an exhaustive key-search attack of the key-exchange protocol using real quadratic fields, we need to ensure that the number ℓ of reduced principal ideals in K is sufficiently large. In this paper we present an example of a family which are not valid for this protocol.

2010 Mathematics Subject Classification. Primary 11R11, 11R16, 11R29; Secondary 11T71.
Key words and phrases. Quadratic field, cubic field, reduced ideal, cryptography.

1. Introduction

In cryptography, a Public key is one of the main techniques for making the internet secure. Most public key crypto-systems are based on intractable computational problems in number theory such as factoring integers. The public key systems have a major advantage over the private key systems, they do not require that the two parties meet beforehand to exchange a key, the circumventing of this problem gave birth to algorithms and key exchange protocols. Since then many public key crypto-systems have been suggested whose security is based on difficult problems in quadratic number fields.

In 1976 Diffie and Hellman introduced their well-known key exchange protocol [5], This scheme is based on the arithmetic in the multiplicative group F^* of a finite field F. In 1988 Buchmann and Williams [1] presented a variant of the Diffie-Hellman key exchange protocol in class groups of imaginary quadratic fields. And in 1989 Buchmann and Williams [3] sketched the other Diffie-Hellman protocol which does not require a group structure. Here we are interested in this latest protocol which is instead based on the infrastructure of a real quadratic field. Currently, the best known algorithms for breaking this scheme are exponential in the size of the key. Moreover, the problem of breaking this scheme is closely related to the very difficult problems of computing class numbers of real quadratic fields and factoring large integers.

In order to raise the degree of security of this scheme, it is necessary that the number ℓ of reduced principal ideals be sufficiently large in the quadratic number field considered $K = \mathbb{Q}(\sqrt{D})$. From Williams [9] we know the following lower bound: $\ell > \frac{R}{\log(D)}$, where R is the regulator of K. moreover, it follows from a result of [7] that $h_K R >> D^{1/2-\eta}$ where $\eta > 0$ arbitrarily small and h_K is the class number of K. To get ℓ large we must therefore find and use real quadratic field with small class numbers. on the other hand it is also necessary to prevent exhaustive attacks, so

Received February 11, 2020. Accepted March 15, 2020.

we must choose real quadratic fields whose cardinal of the cycle of reduced principal ideals is very large.

In this paper we will determine, by the continued fraction algorithm, the cycles of principal reduced ideals of a quadratic fields of type $K = \mathbb{Q}(\sqrt{m^2 \pm 1})$ where m is an integer such that $m^2 \pm 1$ is square-free, and then we find the fundamental unit of these fields, and therefore these fields are not valid for the exchange protocol based on real quadratic fields. We also present, by the Voronoi algorithm a similar results for a pure cubic fields of type $K = \mathbb{Q}(\sqrt[3]{m^3 \pm 1})$ where m is an integer such that $m^3 \pm 1$ is square-free and $\not\equiv \pm 1 \pmod 9$. For this family of pure cubic fields, we will also determine an upper bound of the cardinal of the set $\mathcal{R}$ of principal reduced ideals.

2. Preliminary

Let $K = \mathbb{Q}(\sqrt{D})$ where $D > 1$ is a square free integer. If we denote

$$\sigma = \begin{cases} 1 \text{ if } D \equiv 2, 3 \pmod 4 \\ 2 \text{ if } D \equiv 1 \pmod 4 \end{cases} \quad \text{and } \omega = \frac{\sigma - 1 + \sqrt{D}}{\sigma},$$

then the ring of integers of K is $\mathcal{O} = \mathbb{Z}[\omega]$ and the discriminant of K is $\Delta = \frac{4D}{\sigma^2}$. Let ε_0 be the fundamental unit of K, R its regulator and h_K its class number. We define the norm of $\alpha \in K$ to be $N(\alpha) = \alpha\alpha'$, where α' is the conjugate of α.

Every ideal I of $\mathcal{O}$ has a representation $I = [a, b + c\omega]$ where $a, b, c \in \mathbb{Z}$ such that $a > b \geq 0$, $c > 0$, $c \mid a$, $c \mid b$ and $ac \mid N(b + c\omega)$. Under these conditions the integers a, b, c are unique, further a is the least positive rational integer in I that we denote it by $L(I)$. We call a number $\mu \in I$ a minimum in I if $\mu > 0$ and if there is no $(\alpha \neq 0) \in I$ such that $|\alpha| < \mu$ and $|\alpha'| < |\mu'|$. We note by M_I the set of minimums in I. Because the set $\{\log \mu, \mu \in M_{\mathcal{O}}\}$ is discrete in $\mathbb{R}$, the ordering of minimums in $\mathcal{O}$ can be written as a sequence:

$$\mu_1 = 1 < \mu_2 < \mu_3 < \dots,$$

and since $|N(\mu)| < \frac{2}{\pi} N(I)\sqrt{D}$, there is some $\ell \in \mathbb{N}$ such that

$$\mu_{\ell+1} = \varepsilon_0, \ \mu_{i+j\ell} = \mu_i \varepsilon_0^j, \ \forall (i, j) \in \mathbb{N}^2.$$

We say that the ideal $I = [a, b + c\omega]$ is primitive, if $c = 1$. The ideal I is said to be reduced if I is primitive and $L(I)$ is a minimum in I. For example, $\mathcal{O} = [1, \omega]$ is reduced, $L(\mathcal{O}) = 1$. We denote by $\mathcal{R}$ the set of all reduced principal ideals.

It is known that for every $\mathbf{r} \in \mathcal{R}$ there is a minimum μ in $\mathcal{O}$ such that $\frac{1}{L(\mathbf{r})}\mathbf{r} = \frac{1}{\mu}\mathcal{O}$. The sequence $(\mu_i)_{i \in \mathbb{N}}$ of minimums in $\mathcal{O}$ gives rise to a sequence $(\mathbf{r}_i = (\frac{L(\mathbf{r}_i)}{\mu_i}))_{i \in \mathbb{N}}$ of reduced principal ideals, and since $\mu_{i+j\ell} = \mu_i \varepsilon_0^j$ for all $i, j \in \mathbb{N}$, then $\mathbf{r}_{i+j\ell} = \mathbf{r}_i$ for all $i, j \in \mathbb{N}$, hence $(\mathbf{r}_i)_{i \in \mathbb{N}}$ is purely periodic with length ℓ it follow that the set $\mathcal{R}$ is finite of cardinal ℓ and we have $\mathcal{R} = \{\mathbf{r}_i = (\frac{L(\mathbf{r}_i)}{\mu_i}), 1 \leq i \leq \ell\}$.

For each reduced principal ideal $\mathbf{r}_i$ we associate the distance $\delta_i = \log \mu_i$. We can also define the distance between an ideal $\mathbf{r}_i$ and a positive real number x as follows

$$\delta(\mathbf{r}_i, x) = \delta_i - x.$$

If $x \in \mathbb{R}^+$, then there is a unique $i \in \mathbb{N}$ such that $\delta_i \leq x < \delta_{i+1}$. If $\mathbf{r}_i = (\frac{L(\mathbf{r}_i)}{\mu_i})$ where $\delta_i = \log \mu_i$, then we call $\mathbf{r}_i$ the ideal closest to the left of x and denote it by $\mathbf{r}_{-x}$, and if $\mathbf{r}_{i+1} = (\frac{L(\mathbf{r}_{i+1})}{\mu_{i+1}})$ where $\delta_{i+1} = \log \mu_{i+1}$, then we call $\mathbf{r}_{i+1}$ the ideal closest to the right of x and denote it by $\mathbf{r}_{+x}$.

The idea of the protocol, in brief, is as follows. Alice and Bob publicly agree on a large integer $D > 0$. Alice secretly chooses a positive integer x and computes the reduced principal ideal $\mathbf{a}_{-x}$ and $\delta(\mathbf{a}_{-x}, x)$ and send these two information to Bob. Similarly, Bob secretly chooses a positive integer y and computes the reduced principal ideal $\mathbf{b}_{-y}$ and $\delta(\mathbf{b}_{-y}, y)$ and send these two information to Alice. From x, $\mathbf{b}_{-y}$ and $\delta(\mathbf{b}_{-y}, y)$, Alice computes a reduced principal ideal $\mathbf{c}_{-xy}$. Similarly, using y, $\mathbf{a}_{-x}$ and $\delta(\mathbf{a}_{-x}, x)$, Bob computes a reduced principal ideal $\mathbf{c}_{-xy}$ which is the key.

A part from exhaustive search, The only known way of breaking this protocol is to solve the discrete logarithm problem (DLP) in $\mathcal{R}$, i.e. given a reduced principal ideal $\mathbf{r}_i$ find its distance δ_i. Since $\delta_i = \log \mu_i$ where $\mathbf{r}_i = (\frac{L(\mathbf{r}_i)}{\mu_i}) \in \mathcal{R}$ the DLP in $\mathcal{R}$ is equivalent to the problem of finding for any reduced principal ideal $\mathbf{r}_i$, a generator $\frac{L(\mathbf{r}_i)}{\mu_i}$. For more details concerning this section see [3] and [6].

3. On the choice of D for a real quadratic field

Based on a result of Buchmann and Williams [2], a fast algorithm for solving the DLP in $\mathcal{R}$ can be used to find the regulator R of K. By a result of Schoof [8], we know that if it is possible to find R quickly, then D can be factored quickly. Thus the DLP in $K = \mathbb{Q}(\sqrt{D})$ is at least as difficult as factoring D. On the other hand, to prevent an exhaustive key-search attack, we need to ensure that the number ℓ of reduced principal ideals in $\mathcal{O}$ is sufficiently large, which is not always guaranteed even if D is large as we will see.

Theorem 3.1. *Let $m \geq 1$ be an odd integer such that $D = m^2+1$ is square-free, and let $K = \mathbb{Q}(\sqrt{D})$. Then the only reduced principal ideal in the ring of integers of K is the entire ring* (1).

Proof. We use the notation $\lfloor x \rfloor$ the floor of x, i.e. the largest integer less than or equal to x. If m is an odd integer then $m^2+1 \equiv 2 \pmod 4$ hence $\sigma = 1$ and $\omega = \sqrt{m^2+1}$. Using the continued fraction expansion of ω, we have

$$\omega_0 = \omega = \sqrt{m^2+1} = \frac{P_0 + \sqrt{m^2+1}}{Q_0},$$

$$\omega_1 = \frac{1}{\omega_0 - \lfloor \omega_0 \rfloor} = \frac{1}{\sqrt{m^2+1} - m} = m + \sqrt{m^2+1} = \frac{P_1 + \sqrt{m^2+1}}{Q_1},$$

$$\omega_2 = \frac{1}{\omega_1 - \lfloor \omega_1 \rfloor} = \frac{1}{\sqrt{m^2+1} - m} = \omega_1,$$

hence the length of this sequence is $\ell = 1$, and the ideal correspond to ω_1 is

$$\left[\frac{Q_1}{\sigma}, \frac{P_1 + \sqrt{m^2+1}}{\sigma}\right] = \left[1, m + \sqrt{m^2+1}\right],$$

which is equal to

$$\left[\frac{Q_0}{\sigma}, \frac{P_0 + \sqrt{m^2+1}}{\sigma}\right] = \left[1, \sqrt{m^2+1}\right] = \mathcal{O},$$

which is correspond to ω_0. □

The cycle of reduced ideals of $\mathcal{O}$ is constituted by a only ideal: $\mathcal{R} = \{\mathcal{O}\}$. The minimums of $\mathcal{O}$ are exactly the units of $\mathcal{O}$, and we have

$$\varepsilon_0 = \prod_{i=1}^{\ell} \omega_i = \omega_1 = m + \sqrt{m^2+1}$$

Lemma 3.2. *If $m > 0$ is an even integer then $\lfloor \frac{1+\sqrt{m^2+1}}{2} \rfloor = \frac{m}{2}$.*

Proof. We have $m-1 \leq \sqrt{m^2+1} < m+1$, hence $\sqrt{m^2+1}-1 < m \leq 1+\sqrt{m^2+1}$, it follow that $\frac{1+\sqrt{m^2+1}}{2} - 1 < \frac{m}{2} \leq \frac{1+\sqrt{m^2+1}}{2}$, then $\lfloor \frac{1+\sqrt{m^2+1}}{2} \rfloor = \frac{m}{2}$. □

Theorem 3.3. *Let $m > 2$ be an even integer such that $D = m^2+1$ is square-free, and let $K = \mathbb{Q}(\sqrt{D})$. Then the ring of integers of K has three reduced principal ideals, namely (1), $\left[\frac{m}{2}, \frac{m-1+\sqrt{m^2+1}}{2}\right]$ which is generated by $\frac{m-1+\sqrt{m^2+1}}{2}$, and $\left[\frac{m}{2}, \frac{1+\sqrt{m^2+1}}{2}\right]$ which is generated by $\frac{m+1+\sqrt{m^2+1}}{2}$.*

Proof. If m is an even integer then $m^2+1 \equiv 1 \pmod 4$ hence $\sigma = 2$ and $\omega = \frac{1+\sqrt{m^2+1}}{2}$. We have

$$\omega_0 = \omega = \frac{1+\sqrt{m^2+1}}{2} = \frac{P_0+\sqrt{m^2+1}}{Q_0}$$

which correspond to the ideal

$$I_1 = \left[\frac{Q_0}{\sigma}, \frac{P_0+\sqrt{m^2+1}}{\sigma}\right] = \left[1, \frac{1+\sqrt{m^2+1}}{2}\right] = \mathcal{O}.$$

Then we have

$$\omega_1 = \frac{1}{\omega_0 - \lfloor \omega_0 \rfloor} = \frac{1}{\frac{1+\sqrt{m^2+1}}{2} - \frac{m}{2}} = \frac{m-1+\sqrt{m^2+1}}{m} = \frac{P_1+\sqrt{m^2+1}}{Q_1}$$

which correspond to the ideal

$$I_2 = \left[\frac{Q_1}{\sigma}, \frac{P_1+\sqrt{m^2+1}}{\sigma}\right] = \left[\frac{m}{2}, \frac{m-1+\sqrt{m^2+1}}{2}\right],$$

and I_2 is reduced because we have $\frac{m}{2} < \frac{\sqrt{\Delta}}{2}$, and it's principal because

$$\frac{Q_0}{\omega_1} I_2 = Q_1 I_1 \text{ and } I_2 = \frac{Q_1\omega_1}{Q_0}\mathcal{O} = (\frac{m-1+\sqrt{m^2+1}}{2}).$$

Afterward we have

$$\omega_2 = \frac{1}{\omega_1 - \lfloor \omega_1 \rfloor} = \frac{1}{\frac{m-1+\sqrt{m^2+1}}{m} - 1} = \frac{1+\sqrt{m^2+1}}{m} = \frac{P_2+\sqrt{m^2+1}}{Q_2}$$

which correspond to the reduced ideal

$$I_3 = \left[\frac{Q_2}{\sigma}, \frac{P_2+\sqrt{m^2+1}}{\sigma}\right] = \left[\frac{m}{2}, \frac{1+\sqrt{m^2+1}}{2}\right],$$

and we have

$$\frac{Q_0}{\omega_1\omega_2}I_3 = Q_2I_1 \text{ and } I_3 = \frac{Q_2\omega_1\omega_2}{Q_0}\mathcal{O} = (\frac{m+1+\sqrt{m^2+1}}{2}).$$

We continue this process,

$$\omega_3 = \frac{1}{\omega_2 - \lfloor\omega_2\rfloor} = \frac{1}{\frac{1+\sqrt{m^2+1}}{m} - 1} = \frac{m-1+\sqrt{m^2+1}}{2} = \frac{P_3+\sqrt{m^2+1}}{Q_3},$$

which correspond to the ideal

$$I_4 = \left[1, \frac{m-1+\sqrt{m^2+1}}{2}\right] = \left[1, \frac{m-2}{2} + \frac{1+\sqrt{m^2+1}}{2}\right] = \mathcal{O},$$

this also justified by the fact that $\omega_4 = \omega_1$. □

Remark 3.1. For $m > 2$ an even integer such that $D = m^2+1$ is square-free, we have $\mathcal{R} = \{\mathcal{O}, (\frac{m-1+\sqrt{m^2+1}}{2}), (\frac{m+1+\sqrt{m^2+1}}{2})\}$ and $\varepsilon_0 = \prod_{i=1}^{\ell}\omega_i = \omega_1\omega_2\omega_3 = m + \sqrt{m^2+1}$. For $m = 2$, we have $\mathcal{R} = \{\mathcal{O}\}$ and $\varepsilon_0 = \omega_0 = \frac{1+\sqrt{5}}{2}$.

Theorem 3.4. *Let $m > 1$ be an integer such that $D = m^2 - 1$ is square-free, and let $K = \mathbb{Q}(\sqrt{D})$. Then the ring of integers of K has two reduced principal ideals, namely (1), and $\left[2(m-1), m-1+\sqrt{m^2-1}\right]$ which is generated by $m-1+\sqrt{m^2-1}$.*

Proof. If $m > 1$ is an integer, then $m^2 - 1 \equiv 2, 3 \pmod 4$, therefore $\sigma = 1$, $\omega_0 = \sqrt{m^2-1}$ $(P_0 = 0, Q_0 = 1)$ and we have

$$\omega_1 = \frac{1}{\omega_0 - \lfloor\omega_0\rfloor} = \frac{1}{\sqrt{m^2-1} - (m-1)} = \frac{m-1+\sqrt{m^2-1}}{2(m-1)} = \frac{P_1+\sqrt{m^2-1}}{Q_1},$$

which correspond to the ideal

$$I_2 = \left[\frac{Q_1}{\sigma}, \frac{P_1+\sqrt{m^2-1}}{\sigma}\right] = \left[2(m-1), m-1+\sqrt{m^2-1}\right].$$

Since $2(m-1) < m-1+\sqrt{m^2-1}$ and $-N(I_2) < m-1-\sqrt{m^2-1} < 0$, then I_2 is reduced, and

$$\frac{Q_0}{\omega_1}I_2 = Q_1I_1 = Q_1\mathcal{O}, \text{ and } I_2 = \frac{Q_1\omega_1}{Q_0}\mathcal{O} = (m-1+\sqrt{m^2-1}).$$

We end with

$$\omega_2 = \frac{1}{\omega_1 - \lfloor\omega_1\rfloor} = \frac{1}{\frac{m-1+\sqrt{m^2-1}}{2(m-1)} - 1} = m-1+\sqrt{m^2-1} = \frac{P_2+\sqrt{m^2-1}}{Q_2}$$

which correspond to the ideal $I_3 = \left[1, m-1+\sqrt{m^2-1}\right] = \mathcal{O}$. □

Remark 3.2. For $m > 1$ an integer such that $D = m^2 - 1$ is square-free,we have $\mathcal{R} = \{\mathcal{O}, (m-1+\sqrt{m^2-1})\}$ and $\varepsilon_0 = \prod_{i=1}^{\ell}\omega_i = \omega_1\omega_2 = m + \sqrt{m^2-1}$.

4. On the choice of D for a pure cubic field

It seems that the key-exchange protocol of Buchmann and Williams can be applied in a pure cubic field with the same steps, and hence we need as in the quadratic case a good choice of D.

A pure cubic field is formed by a adjoining $\delta = \sqrt[3]{D}$ to the rationals $\mathbb{Q}$ where D is a cube-free integer. We can assume that $D > 1$, and we can write D in a unique fashion: $D = rs^2$, where $r, s \in \mathbb{N}, \gcd(r, s) = 1$, and r, s are square-free. Moreover we may assume that $r > s$ because if we put $\bar{\delta} = \sqrt[3]{\bar{D}} = \sqrt[3]{r^2 s}$ we have $\mathbb{Q}(\delta) = \mathbb{Q}(\bar{\delta})$. Any such field has one real embedding and a pair of conjugate complex embedding, and hence has one fundamental unit ε_0 and negative discriminant.

The pure cubic number field $K = \mathbb{Q}(\sqrt[3]{D})$ is said to be of type I if $D \not\equiv \pm 1 \pmod 9$, in this case $\left[1, \delta, \bar{\delta}\right]$ is a basis of the ring of integers $\mathcal{O}_K$ of K, and the discriminant of K is $\Delta_K = -27r^2s^2$. Otherwise is said to be of type II and in this case $\left[1, \delta, \frac{1+r\delta+s\bar{\delta}}{3}\right]$ is a basis of $\mathcal{O}_K$, and $\Delta_K = -3r^2s^2$. Denote by α' and α'' the conjugate roots of any $\alpha \in K$. If K is of type I and D is square-free ($s = 1$) then $\mathcal{O}_K = [1, \delta, \delta^2] = \mathbb{Z}[\delta]$ thus we say that K is monogenic.

In the case of a quadratic field we have used the continued fraction algorithm, and the idea can be extended to the Voronoi algorithm in pure cubic field. For a more detailed description of these ideas we refer the reader to [4] and [10].

Let $\delta_1, \delta_2, \delta_3 \in K$ such that

$$\sum_{k=1}^{3} z_k \delta_k = 0 \ (z_k \in \mathbb{Z}) \Leftrightarrow z_1 = z_2 = z_3 = 0.$$

We say that $\mathcal{L} = \{(\omega, \omega', \omega'') \mid \omega = \sum_{k=1}^{3} z_k \delta_k, z_k \in \mathbb{Z}\}$ is a lattice over K with basis $\{\delta_1, \delta_2, \delta_3\}$. Since ω' and ω'' are complex, we consider the real lattice

$$\mathcal{L} = \{\Omega = (\omega, \frac{\omega' - \omega''}{2i}, \frac{\omega' + \omega''}{2}) \mid \omega = \sum_{k=1}^{3} z_k \delta_k, z_k \in \mathbb{Z}\}$$

we also write $\mathcal{L} = \langle \delta_1, \delta_2, \delta_3 \rangle$ and we often identify Ω with to ω and we write $\Omega \approx \omega$.

We say that $(\Theta \approx \theta) \in K$ is a relative minimum of $\mathcal{L}$ if $\Theta \in \mathcal{L}$ and there does not exist $(\Phi \approx \phi \neq 0) \in \mathcal{L}$ such that $|\phi| < |\theta|$ and $\phi'\phi'' < \theta'\theta''$, it is clear that if $\Theta \approx \theta$ then $-\Theta \approx -\theta$ so is, and so we consider that the positive relative minima. If Θ and Φ are relative minima of $\mathcal{L}$ such that $0 < \theta < \phi$ and there does not exist a $\Psi \in \mathcal{L}$ such that $\theta < \psi < \phi$ and $\psi'\psi'' < \theta'\theta''$ we call Φ the relative minimum adjacent to Θ. for any lattice we construct the sequence $(\Theta_n)_{n \in \mathbb{N}}$, where Θ_1 is a minimum of $\mathcal{L}$, and Θ_{k+1} is a relative minimum adjacent to Θ_k.

Now if we consider the lattice $\mathcal{L}_1 = \langle 1, \delta_2, \delta_3 \rangle$ where $[1, \delta_2, \delta_3]$ is an integral basis of $\mathcal{O}_K$, clearly $\Theta_1 = (1, 0, 1)$ is a relative minimum of $\mathcal{L}_1$, and let Θ_2 be the relative minimum adjacent to Θ_1. Put $\theta_g^{(1)} = \theta_2 \approx \Theta_2$ and find $\theta_h^{(1)}$ such that $\mathcal{L}_1 = \langle 1, \theta_g^{(1)}, \theta_h^{(1)} \rangle$. Put $\mathcal{L}_2 = \langle 1, \frac{1}{\theta_g^{(1)}}, \frac{\theta_h^{(1)}}{\theta_g^{(1)}} \rangle$. Again $(1, 0, 1) \approx 1$ is a relative minimum of $\mathcal{L}_2$ and we find $\theta_g^{(2)}$, a relative minimum adjacent to 1 in $\mathcal{L}_2$. We continue like this, we have $(1, 0, 1) \approx 1$ is a relative minimum of $\mathcal{L}_k = \langle 1, \frac{1}{\theta_g^{(k-1)}}, \frac{\theta_h^{(k-1)}}{\theta_g^{(k-1)}} \rangle$ and determining $\theta_g^{(k)}$, the relative minimum adjacent to 1 in $\mathcal{L}_k$. We put $\Theta_{n+1} = \prod_{k=1}^{n} \theta_g^{(k)}$. When for some least integer $k > 1$, $\mathcal{L}_k$ and $\mathcal{L}_1$ are the same lattice, or equivalently, $N(\Theta_k) = 1$, then the sequence of relative minimum of $\mathcal{L}_1$ is

$$\Theta_1 = 1 < \Theta_2 < ... < \Theta_{k-1}$$

and we have

$$\varepsilon_0 = \Theta_k$$

the rest of the sequence is as follows

$$\Theta_k = \varepsilon_0 < \Theta_{k+1} = \Theta_2\varepsilon_0 < ... < \Theta_{2(k-1)} = \Theta_{k-1}\varepsilon_0 < ...$$

Now we will use the correspondence between the lattices of K and the ideals of $\mathcal{O}_K$. Any ideal I of $\mathcal{O}_K = [1, \delta_2, \delta_3]$ has a basis $[\lambda_1, \lambda_2, \lambda_3]$ where $\lambda_1 = a_{11}$, $\lambda_2 = a_{21} + a_{22}\delta_2$ and $\lambda_3 = a_{31} + a_{32}\delta_2 + a_{33}\delta_3$ with $a_{kl} \in \mathbb{Z}$ and $a_{11}, a_{22}, a_{33} > 0$, further a_{11} is the least positive rational integer in I, $(L(I) = a_{11})$. If we put $\mathcal{L} = \langle 1, \frac{\lambda_2}{\lambda_1}, \frac{\lambda_3}{\lambda_1}\rangle$ we say that $\mathcal{L}$ is the 1-lattice which corresponds to the ideal I. If $\mathcal{L}_1 = \alpha\mathcal{L}_2$, $\alpha \in K$ we say that $\mathcal{L}_1$ and $\mathcal{L}_2$ are similar. We call a 1-lattice in which $(1, 0, 1)$ is a relative minimum a reduced lattice. an ideal I is reduced if and only if its corresponding lattice is reduced.

Lemma 4.1. *Let $\mathcal{L}_1$ be a 1-lattice which corresponds to the ideal I_1 and $\mathcal{L}_2$ be a 1-lattice which corresponds to the ideal I_2.*

(1) *If $\mathcal{L}_1 = \alpha\mathcal{L}_2$ then $(L(I_2))I_1 = (L(I_1)\alpha)I_2$.*
(2) *If $I_1 = (\beta)I_2$ then $\mathcal{L}_1 = \frac{L(I_1)}{L(I_2)}\beta\mathcal{L}_2$.*

Proof. Let $I_1 = [L(I_1), \lambda_2, \lambda_3]$ and $I_2 = [L(I_2), \gamma_2, \gamma_3]$, then $\mathcal{L}_1 = \langle 1, \frac{\lambda_2}{L(I_1)}, \frac{\lambda_3}{L(I_1)}\rangle$ and $\mathcal{L}_2 = \langle 1, \frac{\gamma_2}{L(I_2)}, \frac{\gamma_3}{L(I_2)}\rangle$. If $\mathcal{L}_1 = \alpha\mathcal{L}_2$, then there is $M \in GL_3(\mathbb{Z})$ such that

$$\alpha \begin{pmatrix} 1 \\ \gamma_2/L(I_2) \\ \gamma_3/L(I_2 \end{pmatrix} = M \begin{pmatrix} 1 \\ \lambda_2/L(I_1) \\ \lambda_3/L(I_1) \end{pmatrix}$$

hence

$$\frac{\alpha}{L(I_2)} \begin{pmatrix} L(I_2) \\ \gamma_1 \\ \gamma_3 \end{pmatrix} = \frac{1}{L(I_1)} M \begin{pmatrix} L(I_1) \\ \lambda_2 \\ \lambda_3 \end{pmatrix},$$

which proves the first assertion. Similarly we show the second. □

In the remainder of this section we consider the pure cubic field $K = \mathbb{Q}(\delta)$ where $\delta^3 = D$ is a square-free integer and $D \not\equiv \pm 1 \pmod 9$. We will use the correspondence between the lattices of K and the ideals of $\mathcal{O}_K$, to get some important results similar to the ones we got in the quadratic case.

Lemma 4.2. *Let $m \geq 1$ be an integer such that $D = m^3+1$ is square-free and $D \not\equiv \pm 1$ (mod 9), and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then $\Theta \approx m^2 + m\delta + \delta^2$ is a relative minimum of the lattice $\mathcal{L}$ which corresponds to $\mathcal{O}_K$.*

Proof. Let $\Phi \approx \phi \in \mathcal{L}$ such that $|\phi| < |\theta|$ and $\phi'\phi'' < \theta'\theta''$, then $N(\phi) < N(m^2 + m\delta + \delta^2) = 1$, and since $N(\phi) \in \mathbb{Z}$ then $\phi = 0$. □

Theorem 4.3. *Let $m \geq 1$ be an integer such that $D = m^3 + 1$ is square-free and $D \not\equiv \pm 1 \pmod 9$, and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then the only reduced principal ideal of $\mathcal{O}_K$ is $\mathcal{O}_K = (1)$ itself.*

Proof. Let $\mathcal{L}_1$ be the lattice which corresponds to $\mathcal{O}_K$, hence $\mathcal{L}_1 = \langle 1, \delta, \delta^2 \rangle$ where $\delta = \sqrt[3]{m^3 + 1}$. With the same notations above, we have $\Theta_1 = (1, 0, 1) \approx 1$. By the above lemma, $\theta_g^{(1)} = m^2 + m\delta + \delta^2$ is a relative minimum of $\mathcal{L}_1$. If there is $\Psi \approx \psi \in \mathcal{L}_1$ such that

$$1 < \psi = x + y\delta + z\delta^2 < \theta_g^{(1)},\ \frac{1}{4}(2x - y\delta - z\delta^2)^2 + \frac{3}{4}(y\delta - z\delta^2)^2 = \psi'\psi'' < 1,\ (x, y, z) \in \mathbb{Z}^3,$$

then

$$\begin{cases} \frac{-1}{3} < x < \frac{\theta_g^{(1)} + 2}{3} \\ \frac{-1}{\delta\sqrt{3}} < y < \frac{\theta_g^{(1)} + 1 + \sqrt{3}}{3\delta} \\ \frac{-1}{\delta^2\sqrt{3}} < z < \frac{\theta_g^{(1)} + 1 + \sqrt{3}}{3\delta^2} \end{cases} \quad \Rightarrow x, y, z \geq 0.$$

But $z = 0$ means that $\psi = 0$, $z = 1$ means that $\psi = \theta_g^{(1)}$ and $z > 1$ means that the value minimal of ψ (z fixed) is $-2 + 3z\delta^2$ and $\theta_g^{(1)} < -2 + 3z\delta^2$, all these contradict the hypothesis, therefore $\theta_g^{(1)}$ is the relative minimum adjacent to 1 in $\mathcal{L}_1$. We can take $\theta_h^{(1)} = -\delta$ (which is not unique), because

$$\begin{pmatrix} 1 \\ m^2 + m\delta + 1 \\ -\delta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ m^2 & m & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \delta \\ \delta^2 \end{pmatrix},$$

hence $\mathcal{L}_2 = \langle 1, \frac{1}{m^2 + m\delta + \delta^2}, \frac{-\delta}{m^2 + m\delta + \delta^2} \rangle = \langle 1, -m + \delta, m\delta - \delta^2 \rangle$.

We have $\mathcal{L}_2 = \mathcal{L}_1$ because

$$\begin{pmatrix} 1 \\ -m + \delta \\ m\delta - \delta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -m & 1 & 0 \\ 0 & m & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \delta \\ \delta^2 \end{pmatrix},$$

hence the only reduced ideal equivalent to $\mathcal{O}_K$ is itself. □

Corollary 4.4. *Let $m \geq 1$ be an integer such that $D = m^3 + 1$ is square-free and $D \not\equiv \pm 1 \pmod 9$, and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then the fundamental unit of K is*

$$\varepsilon_0 = m^2 + m\sqrt[3]{m^3 + 1} + \sqrt[3]{(m^3 + 1)^2}$$

Proof. We have $\mathcal{L}_2 = \mathcal{L}_1$ hence $\varepsilon_0 = \Theta_2 = \theta_g^{(1)}$. □

Lemma 4.5. *Let $m > 1$ be an integer such that $D = m^3 - 1$ is square-free and $D \not\equiv \pm 1 \pmod 9$, and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then $\Theta \approx m^2 - 1 + m\delta + \delta^2$ is a relative minimum of the lattice $\mathcal{L}$ which corresponds to $\mathcal{O}_K$.*

Proof. Let $\Phi \approx \phi \in \mathcal{L}$ such that $\phi < \theta$ and $\phi'\phi'' < \theta'\theta''$, since $\phi = x + y\delta + z\delta^2$ with $x, y, z \in \mathbb{Z}$, then

$$\begin{cases} 0 \leq x + y\delta + z\delta^2 < m^2 - 1 + m\delta + \delta^2 \\ (\frac{2x - y\delta - z\delta^2}{2})^2 + \frac{3}{4}(y\delta - z\delta^2)^2 < \frac{3m(m-1)}{m^2 - 1 + m\delta + \delta^2} < 1 \end{cases}$$

as in the proof of the later theorem, the integers x, y, z are positive. If we have $z \geq 1$ then $y\delta < m\delta$ or $x < m^2 - 1$ hence $z < \frac{2}{\sqrt{3}\delta^2} + \frac{m}{\delta}$ or $z < \frac{1}{\sqrt{3}\delta^2} + \frac{m^2}{\delta^2}$, in both cases we have $z \leq 1$. if $z = 1$ then $y = m$ and $x = m^2 - 1$ which is not possible therefore $z = 0$ hence $y < \frac{2}{\sqrt{3}\delta} < 1$ and $y = 0$ and this means that $x < 1$ and $x = 0$ finally we have $\phi = 0$. □

Theorem 4.6. *Let $m > 1$ be an integer such that $D = m^3 - 1$ is square-free and $D \not\equiv \pm 1 \pmod 9$, and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then $\mathcal{O}_K$ has two reduced principal ideals, (1) itself and $\left[3m(m-1), 3m(m-1)\delta, (m-1)^2 + (m-1)\delta + \delta^2\right]$ which is principally generated by $-2m^2 + m + 1 + (m-1)\delta + \delta^2$.*

Proof. We consider the lattice $\mathcal{L}_1$ which corresponds to $\mathcal{O}_K$, ($\delta = \sqrt[3]{m^3 - 1}$), where $\Theta_1 = (1, 0, 1) \approx 1$ is a relative minimum. there is no $\Psi \approx \psi \in \mathcal{L}_1$ such that

$$\begin{cases} 1 < \psi = x + y\delta + z\delta^2 < \theta = m^2 - 1 + m\delta + \delta^2, \ (x, y, z) \in \mathbb{Z}^3 \\ \frac{1}{4}(2x - y\delta - z\delta^2)^2 + \frac{3}{4}(y\delta - z\delta^2)^2 = \psi'\psi'' < 1 \end{cases}$$

because the two inequalities means that $z = 0$ hence $\psi = 0$, or $z = 1$ hence $\psi = \theta$, consequently, the relative minimum adjacent to 1 is $\theta_g^{(1)} = m^2 - 1 + m\delta + \delta^2$, and we find $\theta_h^{(1)} = -\delta$ such that $\mathcal{L}_1 = \langle 1, \theta_g^{(1)}, \theta_h^{(1)} \rangle$.

We continue with $\mathcal{L}_2 = \langle 1, \frac{1}{m^2-1+m\delta+\delta^2}, \frac{-\delta}{m^2-1+m\delta+\delta^2} \rangle$ where $(1, 0, 1) \approx 1$ is a relative minimum, and as before we can shown that

$$\theta_g^{(2)} = \frac{(m-1)^2 + (m-1)\delta + \delta^2}{3m(m-1)} = 1 + \frac{1}{m^2 - 1 + m\delta + \delta^2}$$

is the relative minimum adjacent to 1, and we find that

$$\theta_h^{(2)} = \delta \text{ and } \mathcal{L}_2 = \langle 1, \frac{(m-1)^2 + (m-1)\delta + \delta^2}{3m(m-1)}, \delta \rangle.$$

We end with

$$\begin{aligned} \mathcal{L}_3 &= \langle 1, \frac{3m(m-1)}{(m-1)^2 + (m-1)\delta + \delta^2}, \frac{3m(m-1)\delta}{(m-1)^2 + (m-1)\delta + \delta^2} \rangle \\ &= \langle 1, -m + 1 + \delta, (-m+1)\delta + \delta^2 \rangle. \end{aligned}$$

We have $\mathcal{L}_3 = \mathcal{L}_1$ because

$$\begin{pmatrix} 1 \\ -m + 1 + \delta \\ (-m+1)\delta + \delta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -m+1 & 1 & 0 \\ 0 & -m+1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \delta \\ \delta^2 \end{pmatrix}.$$

Finally we have two reduced lattices, namely $\mathcal{L}_1$ and $\mathcal{L}_2$ which correspond respectively to the ideals

$$I_1 = (1) \text{ and } I_2 = \left[3m(m-1), 3m(m-1)\delta, (m-1)^2 + (m-1)\delta + \delta^2\right],$$

and since $\mathcal{L}_2 = \frac{1}{m^2-1+m\delta+\delta^2}\mathcal{L}_1$ then by lemma 4.1 we have

$$I_2 = (\frac{3m(m-1)}{m^2 - 1 + m\delta + \delta^2})I_1 = (-2m^2 + m + 1 + (m-1)\delta + \delta^2).$$

□

Corollary 4.7. *Let $m \geq 1$ be an integer such that $D = m^3 - 1$ is square-free and $\not\equiv \pm 1 \pmod 9$, and let $K = \mathbb{Q}(\sqrt[3]{D})$. Then the fundamental unit of K is*

$$\varepsilon_0 = m^2 + m\sqrt[3]{m^3 - 1} + \sqrt[3]{(m^3 - 1)^2}.$$

Proof. We have $\mathcal{L}_3 = \mathcal{L}_1$, hence $\varepsilon_0 = \Theta_3 = \theta_g^{(2)}\theta_g^{(1)}$. □

If we know the fundamental unit of K, then we can have information on the cardinal of $\mathcal{R}$, indeed we have the following result.

Theorem 4.8. *Let $K = \mathbb{Q}(\delta)$ where $D = \delta^3$ is square-free integer and $D \not\equiv \pm 1 \pmod 9$. If ε_0 is the fundamental unit of K, then the number of principal reduced ideals of $\mathcal{O}_K$ is smaller than $t = \lfloor \frac{\varepsilon_0+1}{3\delta^2} \rfloor \lfloor \frac{\varepsilon_0+1}{3\delta} \rfloor \lfloor \frac{\varepsilon_0+2}{3} \rfloor$.*

Proof. Let $\mu = x + y\delta + z\delta^2$ a minimum of $\mathcal{O}_K$ such that $1 < \mu < \varepsilon_0$, then we have $\mu'\mu'' < 1$ hence $(\frac{2x-y\delta-z\delta^2}{2})^2 + \frac{3}{4}(y\delta - z\delta^2)^2 < 1$, therefore

$$\frac{-1}{\sqrt{3}\delta^2} < z < \frac{\varepsilon_0+1}{3\delta^2} + \frac{1}{\sqrt{3}\delta^2},\ \frac{-1}{\sqrt{3}\delta} < y < \frac{\varepsilon_0+1}{3\delta} + \frac{1}{\sqrt{3}\delta},\ \frac{-1}{3} < x < \frac{\varepsilon_0+2}{3},$$

hence the result. □

Remark 4.1. If there is no minimum μ of $\mathcal{O}_K$ such that $1 < \mu < \varepsilon_0$, then the only reduced principal ideal in $\mathcal{O}_K$ is $\mathcal{O}_K$ itself.

References

[1] J.A. Buchmann and H.C. Williams, A key exchange system based on imaginary quadratic fields, *Journal of Cryptology* **1** (1988), 107–118.

[2] J.A. Buchmann and H.C. Williams, Quadratic fields and cryptography, In: J.H. Loxton (ed.) *Number Theory and Cryptography*, Cambridge University Press, Cambridge (1990), 9–25.

[3] J.A. Buchmann, R. Scheidler, and H.C. Williams, A key exchange protocol using real quadratic fields, *Journal of cryptology* **7** (1994), no. 3, 171–199.

[4] B.N. Delone and D.K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Transi. Math. Mono. **10**, AMS, Providence, R.I., 1964.

[5] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), no. 6, 644–654.

[6] R.A. Mollin, *Quadratics*, CRC Press, Boca Raton-New York-London-Tokyo, 1996.

[7] R.A. Mollin and H.C. Williams, Computation of the class number of a real quadratic field, *Utilitas Math.* **41** (1992), 259–308.

[8] R. Schoof (1983), Quadratic fields and factorization, In: H.W. Lenstra jr., R. Tijdeman (eds.)*Computational Methods in Number Theory*, MC-Tracts **154/155**, Part II, Amsterdam (1982), 235–286.

[9] H.C. Williams, Continued fractions and number-theoretic computations, *The Rocky Mountain Journal of Mathematics* **15** (1985), no. 2, 621–655.

[10] H.C. Williams, G. Cormack, and E. Seah, Calculation of the regulator of a pure cubic field, *Mathematics of Computation* **34** (1980), no. 150, 567–611.

(Abdelmalek Azizi, Jamal Benamara, Moulay Chrif Ismaili) Department of Mathematics, Faculty of Sciences, Mohammed First University, 60000 Oujda, Morocco
E-mail address: abdelmalekazizi@yahoo.fr, benamarajamal@hotmail.fr, mcismaili@yahoo.fr

(Mohammed Talbi) Regional center of Education and Training, 60000 Oujda, Morocco
E-mail address: talbimm@yahoo.fr