Sciencia Acta Xaveriana
An International Science Journal
ISSN. 0976-1152

Volume 5
No. 1
pp. 1-14
March 2014

Pell's equations $x^2 - df^2y^2 = \pm 1, \pm 4$ and continued fraction expansion of a quadratic irrational

Lionel Bapoungué
Université de Yaoundé 1
École normale supérieure
BP 47 Yaoundé - Cameroun
Email : lbapoungue@hotmail.com

Abstract

Let $K = \mathbb{Q}(\sqrt{d})$, the real quadratic field associated with the positive square-free integer d, $\mathcal{O}_K$ its maximal order and $\mathcal{O}_f$ an order of index f in K. Let $u + vf\omega \in \mathcal{O}_f$ be and write $-f\omega^\sigma = [u_0, \overline{u_1, ..., u_t}]$ for the continued fraction expansion of $-f\omega^\sigma$, where ω^σ is the conjugate of ω. We prove that if $u + vf\omega$ is a unit of $\mathcal{O}_f$, then $\frac{u}{v}$ is a reduced of $-f\omega^\sigma$. This property allows the determination of the group of units of $\mathcal{O}_f$. With the former group, we give a description of the family of all the solutions of each separate equation $x^2 - df^2y^2 \equiv \pm 1$ and $x^2 - df^2y^2 \equiv \pm 4$.

2010 Mathematics Subject Classifications : 11D09, 11J68, 11J86.

Keywords and Phrases : Diophantine equations, Quadratic forms, continued fractions, units.

(Received : February 2014; Accepted March 2014)

Introduction

denotes a positive square-free integer (therefore $d \notin 4\mathbb{Z}$). When we
ons of the Pell's equation

.1) $$x^2 - df^2y^2 = 1,$$

here f is an integer ≥ 1, one begins to solve the problem concerning

.2) $$x^2 - dy^2 = 1,$$

d one determines the solutions (α, β) of (1.2) such that f divides α.
method used by the author of [10] and [11].
nother equivalent method to formulate that point-of-view is as foll
$= \mathbb{Q}(\sqrt{d})$, the real quadratic field associated with the positive squar

integer d, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ its maximal order with

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d}, & \text{if } d \equiv 2 \text{ ou } 3 \pmod 4 \end{cases}$$

and $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\omega$ an order of index f in K. One begins to determine the fundamental unit ε of norm 1 of $\mathcal{O}_f$ and one seeks the integers n such that ε^n is a unit relatively in $\mathcal{O}_f$. Commonly, equation (1.2) is known as *Pell's equation* ; but this is unjustified since Pell did not make any independent contribution to the subject. References to indeterminate equations of the Pell type occur throughout the history of mathematics. The most interesting example arises with the Indian mathematician **Brahmagupta** who studies in the 7-th century, the equation $y^2 = ax^2 + 1$, where a is an integer ; another Indian mathematician of the 12-th century, namely **Bhāskara**, had been continued the works of Brahmagupta [5] : hc has givcn particular solutions of thc cquation $x^2 = 1 + py^2$ for $p = 8, 11, 32, 61$ and 67 ; by example, when $x^2 = 1 + 61y^2$, he gets the solution $(x, y) = (17776319049, 22615390)$. That's why, the history of the Pell's equation is ambiguous. In paper [8], the author has used the length $l(\alpha)$ of the period of a continued fraction expansion of the quadratic irrational number α to solve the Pell's equations

$$x^2 - dy^2 = -1, \ -4.$$

Definition 1 - *A real irrational number is called a* ***quadratic irrational*** *if it is a root of a quadratic equation*

$$a\alpha^2 + b\alpha + c = 0$$

where a, b, c are integers with $a > 0$.

The quadratic equation of definition 1 has roots

(1.3) $$\alpha = \frac{-b+\sqrt{b^2-4ac}}{2a} = \frac{P+\sqrt{D}}{Q}$$

and

(1.4) $$\alpha' = \frac{-b-\sqrt{b^2-4ac}}{2a} = \frac{P-\sqrt{D}}{Q}$$

where

$$P = -b, \ D = b^2 - 4ac, \ Q = 2a > 0$$

are integers. If we assume that $D > 0$ is not a perfect square, then the roots α and α' are quadratic surds [**9**, Chapter two] of the form $A \pm B\sqrt{D}$ where $A = \frac{P}{Q}$ and $B = \frac{1}{Q}$ are rational.

Under this assumptions, we state :

Definition 2 - *The quadratic irrational* α *given by* (1.3) *is said to be* ***reduced*** *if* α *is greater than* 1 *and if its conjugate* α' *denotes* α^σ, *given by* (1.4), *lies between* -1 *and* 0 *:*

$$\alpha > 1 \quad and \quad -1 < \alpha^\sigma < 0.$$

A reference of continued fraction is found in the works of the Indian mathematician **Āryabhata**, who died around 550 A.D [5]. His work contains one of the earliest attempts at the general solutions of a linear equation $ax+by=c$ by the use of continued fractions, that's why, like the Pell's equation, the earliest traces of the idea of a continued fraction are somewhat confused. Further traces of the general concept of a continued fraction are found occasionally in Arab and Greek writings. It is well-known that :

Proposition 3 - [**7**, *Chapter V*] (*see also* [**9**, *Chapter one*]) *Let* $x \in \mathbb{R}_+^*$ *be and* $x=[u_0,u_1,...]$ *its continued fraction expansion. Then :*

(i) the n-th reduced $\frac{p_n}{q_n}=[u_0,...,u_n]$ *is a reducible fraction, where*

$$p_{-2}=0,\ \ p_{-1}=1,\ p_n=p_{n-1}u_n+p_{n-2}$$

$$q_{-2}=0,\ \ q_{-1}=1,\ q_n=q_{n-1}u_n+q_{n-2}\ ;$$

(ii) $[u_0,...,u_n,x]=\widetilde{H}_n(x)$ *with*

$$\widetilde{H}_n(x)=\frac{p_nx+p_{n-1}}{q_nx+q_{n-1}}$$

and

$$\widetilde{H}_n^{-1}(x)=\frac{q_{n-1}x-p_{n-1}}{-q_nx+p_n},\ \ \widetilde{H}_n(x_{n+1})=x,\ \ x_n=u_n+\frac{1}{x_{n+1}}.$$

Theorem 4 ***(Legendre)*** *If the rational* $\frac{p}{q}$ *verifies* $\left|x-\frac{p}{q}\right|<\frac{1}{2q^2}$, *then* $\frac{p}{q}$ *is a reduced of* x.

Proposition 5 ***(Legendre)*** *Let* $K=\mathbb{Q}(\sqrt{d})$, *the real quadratic field associated with the positive square-free integer* d, $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\omega$ *its maximal order and* $\mathcal{O}_f=\mathbb{Z}+\mathbb{Z}f\omega$ *an order of index* f *in* K *of discriminant*

$$D=Disc(\mathcal{O}_f)=f^2Disc(\mathcal{O}_K)$$

with

$$Disc(\mathcal{O}_K)=\begin{cases} d, & if\ \ d\equiv 1 \pmod 4 \\ 4d, & if\ d\equiv 2\ ou\ 3 \pmod 4. \end{cases}$$

Write

$$-f\omega^\sigma=[u_0,\overline{u_1,...,u_t}]$$

for the continued fraction expansion of $-f\omega^\sigma$. *If* $\frac{p_n}{q_n}$ *is the n-th reduced of* $-f\omega^\sigma$, *then* $p_{t-1}+q_{t-1}f\omega$ *is a unit of* $\mathcal{O}_f$ *of norm* $\mathcal{N}(p_{t-1}+q_{t-1}f\omega)=(-1)^t$.

Proposition 3, theorem 4 and proposition 5 had led us in papers [1], [2] and [3] to solve some Diophantine equations. In this paper, we shall be concerned with thc solvability of thc Pell's cquations

(1.5) $$x^2-df^2y^2=\pm 1,$$

and

(1.6) $$x^2 - df^2y^2 = \pm 4.$$

Our method uses the continued fraction expansion of $-f\omega^\sigma$. In section 2, we show that if $-f\omega^\sigma = [u_0, \overline{u_1, ..., u_t}]$ is the continued fraction expansion of $-f\omega^\sigma$, then $-f\omega^\sigma$ is not in general reduced (Lemma 9). In the remainder of section 2, assuming that $u + vf\omega$ is a unit of $\mathcal{O}_f$, we use proposition 3 and theorem 4 to prove that $\frac{u}{v}$ is a reduced of $-f\omega^\sigma$ (Lemma 10). In section 3, we seek the units of the ring $\mathcal{O}_f$ (Theorems 11, 13 and 14) by the use of the results of section 1 and 2, the discussion involving the following result proved in [6].

Lemma 6 - *Let G be a subgroup of multiplicative group $(\mathbb{R}_+^*, .)$. Let $\mathcal{U} = \{g \in G : g > 1\}$ admitting a smallest element α. Then*

$$G = \{\alpha^n \in G : n \in \mathbb{Z}\}.$$

In section 4, we give the description of the family of solutions for each separate equation of (1.5) and (1.6) (Theorems 16 and 19) by the same arguments as in the results of section 3. The paper is concluded in section 5 with some numerical examples.

2 Some lemmas concerning continued fraction expansion of $-f\omega^\sigma$

Lemma 7 - *Let $x \in \mathbb{R}_+^*$ be. If $x = [u_0, u_1, ...]$ is the continued fraction expansion of x, then*

$$\frac{1}{x} = [0, u_0, u_1, ...] = [v_0, v_1, ...].$$

Proof. First, according to proposition 3, write :
H_n for the matrix associated to x,
K_n for the matrix associated to $\frac{1}{x}$.
Let $\frac{p_n}{q_n}$ and $\frac{r_n}{s_n}$ be the respective reduced of x and $\frac{1}{x}$.
Next, set :

$$K_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } K_1 = K_0H_0 ;$$

whence by induction we have $K_{n+1} = K_0H_n$; then, with (ii) of proposition 3, we have $\widetilde{H}_n(+\infty) = \frac{p_n}{q_n}$ therefore, taking $\widetilde{K}_0$ on both sides of that last relation, we deduce that

$$\widetilde{K}_{n+1} = \widetilde{K}_0 \left(\frac{p_n}{q_n}\right)$$

that is to say $\frac{r_{n+1}}{s_{n+1}} = \frac{q_n}{p_n}$. ■

Lemma 8 - *Let $K = \mathbb{Q}(\sqrt{d})$, the real quadratic field associated with the positive square-free integer d, $\mathcal{O}_K$ its maximal order and $\mathcal{O}_f$ an order of index f in K of discrminant $D = f^2 Disc(\mathcal{O}_K)$. Let*

$$-f\omega^\sigma = [u_0, \overline{u_1, ..., u_t}]$$

be the continued fraction expansion of $-f\omega^{\sigma}$. *If for* $1 \leq i < t$, $x_i = \frac{b_i + \sqrt{D}}{2a_i}$ *is the i-th complete quotient of* $-f\omega^{\sigma}$, *then* $a_i \neq 1$.

Proof. Assume that for $i \geq t$, $a_i = 1$. Then, we have :

$$x_i = \frac{b_i + \sqrt{D}}{2a_i} = \frac{b_i + \sqrt{D}}{2} = \frac{-fTr\omega + \sqrt{D}}{2} + \frac{b_i + fTr\omega}{2} = x_0 + \frac{b_i + fTr\omega}{2}$$

hence

$$u_i = [x_i] = [x_0] + \frac{b_i + fTr\omega}{2} = u_0 + \frac{b_i + fTr\omega}{2}$$

where the square bracket $[u]$ means the integral part of u, and $x_i - u_i = x_0 - u_0$ so that $x_{i+1} = x_1$ contradicting the fact that t is the period. ■

Lemma 9 - *Let* $K = \mathbb{Q}(\sqrt{d})$, *the real quadratic field associated with the positive square-free integer* d, *and* $\mathcal{O}_f$ *an order of index* f *in* K. *If*

$$-f\omega^{\sigma} = [u_0, \overline{u_1, ..., u_t}]$$

is the continued fraction expansion of $-f\omega^{\sigma}$, *then in general,* $-f\omega^{\sigma}$ *is not reduced.*

Proof. We have $-f\omega^{\sigma} = u_0 + \frac{1}{x_1}$ hence $x_1 = \frac{-1}{f\omega^{\sigma} + u_0}$; but $x_1^{\sigma} = \frac{-1}{f\omega + u_0} < 0$ because $u_0 + f\omega > 0$ and, since $u_0 + f\omega \geq f\omega \geq \omega > 1$, we have $\mid x_1^{\sigma} \mid = \frac{1}{f\omega + u_0} < 1$. Therefore

$$\omega = \begin{cases} \sqrt{d} \geq \sqrt{2} > 1, \text{ if } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} \geq \frac{1+\sqrt{5}}{2} > 1, \text{ if } d \equiv 1 \pmod 4, \end{cases}$$

showing that $-f\omega^{\sigma} > 1$. Now, set $x = -f\omega^{\sigma}$. Then,

$$x^{\sigma} = f\omega = \begin{cases} -f\sqrt{d}, \text{ if } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \frac{f(1-\sqrt{d})}{2}, \text{ if } d \equiv 1 \pmod 4. \end{cases}$$

Therefore, x^{σ} is negative. Moreover,

$$-1 < x^{\sigma} < 0 \Leftrightarrow \begin{cases} f\sqrt{d} < 1, \text{ if } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \frac{f(\sqrt{d}-1)}{2} < 1, \text{ if } d \equiv 1 \pmod 4. \end{cases}$$

The first case is impossible. In the second case, since $d \equiv 1 \pmod 4$, we have $\sqrt{d} \geq \sqrt{5} > 2$ and as $\frac{f(\sqrt{d}-1)}{2} < 1$, we have $f\sqrt{d} < f + 2 \Rightarrow 2f < f + 2$ i.e. $f < 2$ therefore $f = 1$, whence $\sqrt{d} < 3$ and necessary $d = 5$ proving that in general, $-f\omega^{\sigma}$ is not reduced. ■

Lemma 10 - *With the notations and hypotheses of lemma 9, let* $u + vf\omega \in \mathcal{O}_f$ *be. If* $u + vf\omega$ *is a unit of* $\mathcal{O}_f$, *then* $\frac{u}{v}$ *is a reduced of* $-f\omega^{\sigma}$.

Proof. Assume that $\frac{u}{v} > -f\omega^\sigma$; then we have

$$\left|-f\omega^\sigma - \frac{u}{v}\right| = \frac{|u + vf\omega^\sigma|}{v} = \frac{1}{v\,|u + vf\omega|}.$$

If $\frac{u}{v} = f\omega > 2$, then

$$\left|-f\omega^\sigma - \frac{u}{v}\right| = \frac{1}{v\,|u + vf\omega|} < \frac{1}{2v^2}.$$

Thus $\frac{u}{v} + f\omega > -\omega^\sigma + f\omega \geq -\omega^\sigma + \omega$. But

$$\omega - \omega^\sigma = \begin{cases} 2\sqrt{d} \geq 2, \text{ if } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \sqrt{d} \geq \sqrt{5} > 2, \text{ if } d \equiv 1 \pmod 4. \end{cases}$$

Therefore, in every case $\omega - \omega^\sigma > 2$ and theorem 4 shows that $\frac{u}{v}$ is a reduced of $-f\omega^\sigma$.

Now, assume that $\frac{u}{v} < -f\omega^\sigma$; then we can write :

$$\left|-f\omega^\sigma - \frac{u}{v}\right| = \left|\frac{-1}{f\omega^\sigma} - \frac{v}{u}\right| = \frac{|u + vf\omega^\sigma|}{|uf\omega^\sigma|} = \frac{1}{u\,|f\omega^\sigma|\,|u + vf\omega|}.$$

But since

$$-f\omega^\sigma + \frac{v}{u}(-f\omega^\sigma)f\omega > -f\omega^\sigma + f\omega \geq \omega - \omega^\sigma \geq 2$$

and as

$$|f\omega^\sigma|\left|1 + \frac{v}{u}f\omega\right| = -f\omega^\sigma + \frac{v}{u}(-f\omega^\sigma)f\omega$$

we get

$$\frac{1}{u\,|f\omega^\sigma|\,|u + vf\omega|} < 2.$$

Therefore theorem 4 shows that $\frac{u}{v}$ is a reduced of $-\frac{1}{f\omega^\sigma}$. It follows that, from lemma 7, $\frac{u}{v}$ is a reduced of $-f\omega^\sigma$. Therefore, in the two cases, $\frac{u}{v}$ is a reduced of $-f\omega^\sigma$. ■

3 The finding of the real units of $\mathcal{O}_f$

In the ensuing of this work, we shall write $\mathcal{O}_f^\times$ for the goup of units of $\mathcal{O}_f$ and in view of proposition 5,

$$\gamma_f = p_{t-1} + q_{t-1}f\omega.$$

Theorem 11 - *Let $K = \mathbb{Q}(\sqrt{d})$, the real quadratic field associated with the positive square-free integer d, $\mathcal{O}_f$ an order of index f in K and*

$$-f\omega^\sigma = [u_0, \overline{u_1, ..., u_t}]$$

the continued fraction expansion of $-f\omega^\sigma$. If $\frac{p_{t-1}}{q_{t-1}}$ is its $(t-1)$-th reduced and if γ_f is a unit of $\mathcal{O}_f$ of norm $\mathcal{N}(\mathcal{O}_f) = (-1)^t$, then γ_f is the smallest unit greater than one of $\mathcal{O}_f$.

Proof. Let γ be a unit of $\mathcal{O}_f$. Write γ for $\gamma = u + vf\omega$. Then we have

$$\omega - \omega^\sigma = \begin{cases} 2\sqrt{d}, \text{ if } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \sqrt{d}, \text{ if } d \equiv 1 \pmod 4. \end{cases}$$

Therefore

$$\gamma - \gamma^\sigma = \gamma \pm \frac{1}{\gamma} > 0 \ ;$$

this implies $vf(\omega - \omega^\sigma) > 0$, so that $v > 0$.

Let us show now that $u > 0$. We have :

$$\frac{1}{\gamma} = \mid \gamma^\sigma \mid = \mid u + vf\omega^\sigma \mid < 1 \Rightarrow u > -1 - vf\omega^\sigma \ ;$$

from this, we deduce that $u > 0$ except only in the case : $f \neq 1$ or $d \neq 5$. In this case, since from the proof of lemma 9 $f\omega^\sigma \leq -1$, we have $u > -1 - vf\omega^\sigma \geq -1 + v \geq 0$ so that $u > 0$.

Now, when $f = 1$ and $d = 5$, we have :

$$u > -1 + v\left(\frac{\sqrt{5}-1}{2}\right).$$

If $v \geq 2$, then $u > -1 + \sqrt{5} - 1 = \sqrt{5} - 2 > 0$;

If $v = 1$, then $u > -1 + \frac{\sqrt{5}-1}{2} = \frac{\sqrt{5}-3}{2} \simeq -0.38$; therefore $u \geq 0$, but if $u = 0$, we have $vf\omega \in \mathcal{O}_f^\times$.

It follows that $u > 0$, $v > 0$ except when $d = 5$ and $f = 1$. Thus, taking $G = \mathcal{O}_f^\times$ and $\gamma = g$ in lemma 6, we see that there is in $\mathcal{U}$ a smallest unit $\gamma_f > 0$. Write γ_f for $\gamma_f = r + sf\omega$ with $r, s > 0$. But, from lemma 10, $\frac{r}{s}$ is a reduced of $-f\omega^\sigma$ of period t. Since $\frac{p_{t-1}}{q_{t-1}}$ is its $(t-1)$-th reduced, we have $\gcd(p_{t-1}, q_{t-1}) = 1$. It remains to show that $r = p_{t-1}$, $s = q_{t-1}$. Let $d = \text{pgcd}(r, s)$; then we may write :

$$r = dr', s = ds' \ ;$$

whence, $\gamma_f = d(r' + s'f\omega)$. But, according to proposition 5, $\gamma_f \in \mathcal{O}_f^\times$ is of norm $(-1)^t$, therefore

$$\mathcal{N}(\gamma_f) = d^2\mathcal{N}(r' + s'f\omega) = \pm 1$$

which implies $d = 1$. Hence, necessarely we have $r = p_{t-1}$, $s = q_{t-1}$ so that $\gamma_f = p_{t-1} + q_{t-1}f\omega > 1$. This proves that γ_f is the smallest unit of $\mathcal{O}_f$ which is greater than one. ■

Definition 12 - $\gamma_f = p_{t-1} + q_{t-1}f\omega$ *is called the* ***fundamental unit of*** $\mathcal{O}_f$.

With lemma 6 and the proof of theorem 11, we may write :

$$\mathcal{U} = \left\{\gamma \in \mathcal{O}_f^\times : \gamma > 1\right\}.$$

Theorem 13 - *With the same notations and hypotheses as in theorem 11, every unit $\gamma > 1$ is expressed in the form*

$$\gamma = \gamma_f^n = p_{nt-1} + q_{nt-1} f\omega, \quad n \geq 1.$$

Proof. Let γ be a unit of $\mathcal{O}_f$ and write γ for $\gamma = u + vf\omega$. Since from lemma 10, $\frac{u}{v}$ is a reduced of $-f\omega^{\sigma}$, there exists an integer $n \geq 0$ such that $\frac{u}{v}$ is the reduced $\frac{p_n}{q_n}$. But γ_f is the fundamental unit of $\mathcal{O}_f$, therefore

$$\mathcal{N}(\gamma_f) = \pm 1 = \mathcal{N}(p_n + q_n f\omega) = (-1)^{n-1} a_{n-1}$$

which implies that $a_{n-1} = 1$ and lemma 7 imposes that $n = t, 2t, ..., kt, ...$ showing that

$$\mathcal{U} \subseteq \{p_{nt-1} + q_{nt-1} f\omega, \quad n \geq 1\}$$

(with $d = 5, f = 1, u = 0, v = 1$). As all these numbers are in $\mathcal{U}$, we have the equality

$$\mathcal{U} = \{p_{nt-1} + q_{nt-1} f\omega, \quad n \geq 1\}.$$

Finally, the two sequences $(\gamma_f^n)_{n \geq 1}$ and $(p_{nt-1} + q_{nt-1} f\omega)_{n \geq 1}$ are strictly increasing so that necessarely $\gamma = \gamma_f^n = p_{nt-1} + q_{nt-1} f\omega, \quad n \geq 1$. ■

Theorem 14 -*The group of real units of $\mathcal{O}_f$ is :*

$$\mathcal{O}_f^{\times} = \{\pm (p_{t-1} + q_{t-1} f\omega)^n : n \in \mathbb{Z}\}.$$

Proof. Let $\gamma \in \mathcal{O}_f^{\times}$ be. If :

· $\gamma \geq 1$, then with theorem 13, we see that $\gamma = (p_{t-1} + q_{t-1} f\omega)^n, \ n \geq 0$.

· $0 < \gamma < 1$, then $\frac{1}{\gamma} \in \mathcal{O}_f^{\times}$ and $\frac{1}{\gamma} > 1$ therefore $\frac{1}{\gamma} = (p_{t-1} + q_{t-1} f\omega)^n$, $n \geq 1$ and $\gamma = (p_{t-1} + q_{t-1} f\omega)^m, \ m \leq -1$.

· $\gamma < 0$, then $-\gamma \in \mathcal{O}_f^{\times}$ and $-\gamma > 0$ so that $\gamma = -(p_{t-1} + q_{t-1} f\omega)^n$, $n \in \mathbb{Z}$. ■

Remark 15 - $\mathcal{O}_f^{\times}$ *can be written also as :*

$$\mathcal{O}_f^{\times} = \pm (p_{t-1} + q_{t-1} f\omega)^{\mathbb{Z}}.$$

4 Description of solutions of Pell's equations (1.5) and (1.6)

In this section, we give the family of solutions of each separate equation of equations (1.5) and (1.6).

4.1 Equation (1.5)

Theorem 16 - *Let d and f be two integers ≥ 1 with square-free d. If $d \equiv 2$ or 3 (mod 4) and if*

$$f\sqrt{d} = [u_0, \overline{u_1, ..., u_t}],$$

is the continued fraction expansion of $f\sqrt{d}$ in which $\frac{p_{t-1}}{q_{t-1}}$ is the $(t-1)$-th reduced, then equation (1.5) has always the solution $p_{t-1} + q_{t-1}f\sqrt{d}$ and all its solutions are given by

$$x + yf\sqrt{d} = \pm(p_{t-1} + q_{t-1}f\sqrt{d})^n,\ n \in \mathbb{Z}.$$

Proof. Since $d \equiv 2$ or 3 (mod 4), it is well-known in section 1 that $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\sqrt{d}$ is an order of the quadratic field K. As $\frac{p_{t-1}}{q_{t-1}}$ is the $(t-1)$-th reduced of $-f(-\sqrt{d})$, by proposition 5, $\gamma_f = p_{t-1} + q_{t-1}f\sqrt{d} \in \mathcal{O}_f^\times$ and theorem 11 shows that γ_f is the smallest unit greater than one of $\mathcal{O}_f$ so that

$$\mathcal{N}(p_{t-1} + q_{t-1}f\sqrt{d}) = p_{t-1}^2 + q_{t-1}^2 f^2 d = \pm 1.$$

This proves that the pair $(p_{t-1}, q_{t-1}f)$ is a solution of (1.5). Therefore with theorem 14, we see that the solutions in integers numbers (x, y) of (1.5) are obtained as follows : take the fundamental unit $p_{t-1} + q_{t-1}f\sqrt{d} \in \mathcal{O}_f$ and put

$$x + yf\sqrt{d} = \pm(p_{t-1} + q_{t-1}f\sqrt{d})^n,\ n \in \mathbb{Z}.$$

The solution (x, y) lists all the solutions of (1.5). ■

Definition 17 - *The solution $(p_{t-1}, q_{t-1}f)$ or $p_{t-1} + q_{t-1}f\sqrt{d}$ is called the* ***fundamental*** *(or* ***the minimal*****) solution** *of equation (1.5).*

Remark 18 - *It is clear that, if the fundamental unit of $\mathcal{O}_f$ is of norm 1, (x, y) is a solution of equation (1.1) ; then the equation*

(4.1) $$x^2 - df^2y^2 = -1$$

has no solution. But if the fundamental unit of $\mathcal{O}_f$ is of norm -1, then the solutions of (1.1) are of the form

$$x + yf\sqrt{d} = \pm(p_{t-1} + q_{t-1}f\sqrt{d})^{2n},\ \ n \in \mathbb{Z}$$

and those of (4.1) of the form

$$x + yf\sqrt{d} = \pm(p_{t-1} + q_{t-1}f\sqrt{d})^{2n+1},\ \ n \in \mathbb{Z}.$$

4.2 Equation (1.6)

Theorem 19 - *Let d and f be two integers ≥ 1 with square-free d. If $d \equiv 1$ (mod 4) and if*

$$f\frac{\sqrt{d}-1}{2} = [u_0, \overline{u_1, ..., u_t}],$$

is the continued fraction expansion of $f\frac{\sqrt{d}-1}{2}$ *in which* $\frac{p_{t-1}}{q_{t-1}}$ *is the* $(t-1)$*-th reduced, then equation* (1.6) *has always the solution* $\frac{1}{2}(2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d})$ *and all its solutions are given by*

$$\frac{x+yf\sqrt{d}}{2} = \pm\left(\frac{2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d}}{2}\right)^n, \quad n \in \mathbb{Z}.$$

Proof. Since $d \equiv 1 \pmod 4$, it is well-known that $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\frac{\sqrt{d}+1}{2}$ is an order of the quadratic field K. As $\frac{p_{t-1}}{q_{t-1}}$ is the $(t-1)$-th reduced of $-f\frac{1-\sqrt{d}}{2}$, by proposition 5, $\gamma_f = \frac{1}{2}(2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d}) \in \mathcal{O}_f^\times$ and theorem 11 shows that γ_f is the smallest unit greater than one of $\mathcal{O}_f$ so that

$$\mathcal{N}\left(p_{t-1}+q_{t-1}f\frac{1+\sqrt{d}}{2}\right) = p_{t-1}^2 + p_{t-1}q_{t-1}f + q_{t-1}^2f^2\left(\frac{1-d}{4}\right) = \pm 1,$$

that is to say

$$\left(\frac{2p_{t-1}+q_{t-1}f}{2}\right)^2 - \left(\frac{q_{t-1}f}{2}\right)^2 d = \pm 1.$$

This proves that the pair $\left(\frac{2p_{t-1}+q_{t-1}f}{2}, \frac{q_{t-1}f}{2}\right)$ is a solution of (1.6).

Conversely, if (x,y) is an integer solution of (1.6), then $\frac{1}{2}(x+yf\sqrt{d}) \in \mathcal{O}_f$ (its trace is x and its norm, by (1.6), is ± 1) and hence a unit of $\mathcal{O}_f$. As in the proof of theorem 16, writing $\frac{1}{2}(2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d})$ for the fundamental unit of $\mathcal{O}_f$, we see that with theorem 14, the solutions in pairs of integers numbers (x,y) of (1.6) are given by

$$\frac{x+yf\sqrt{d}}{2} = \pm\left(\frac{2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d}}{2}\right)^n, \quad n \in \mathbb{Z}.$$

The solution (x,y) lists all the solutions of (1.6). ■

Definition 20 - *The solution* $\frac{1}{2}(2p_{t-1}+q_{t-1}f+q_{t-1}f\sqrt{d})$ *or* $\left(\frac{2p_{t-1}+q_{t-1}f}{2}, \frac{q_{t-1}f}{2}\right)$ *is called the* ***fundamental*** *(or* ***the minimal) solution*** *of equation (1.6).*

Remark 21 - *The same as in remark 18, replacing* ± 1 *by* ± 4.

5 Numerical examples

Example 1. Take $d = 6$. Then $d \equiv 2 \pmod 4$ is square-free such that $\mathbb{Q}(\sqrt{6})$ is a quadratic field. To find the fundamental unit of the order $\mathcal{O}_7 = \mathbb{Z}+\mathbb{Z}\left[7\sqrt{6}\right]$ of the field $\mathbb{Q}(\sqrt{6})$, we begin by develop the number $-7\omega^\sigma = 7\sqrt{6} = \sqrt{294}$ in continued fraction. We have :

$\sqrt{294} = 17 + (\sqrt{294} - 17),\ u_0 = 17$
$\frac{1}{\sqrt{294}-17} = \frac{\sqrt{294}+17}{5} = 6 + \frac{\sqrt{294}+13}{5},\ u_1 = 6$
$\frac{5}{\sqrt{294}-13} = \frac{5(\sqrt{294}+13)}{125} = \frac{\sqrt{294}+13}{25} = 1 + \frac{\sqrt{294}-12}{25},\ u_2 = 1$
$\frac{25}{\sqrt{294}-12} = \frac{25(\sqrt{294}+12)}{150} = \frac{\sqrt{294}+12}{6} = 4 + \frac{\sqrt{294}-12}{6},\ u_3 = 4$
$\frac{6}{\sqrt{294}-12} = \frac{6(\sqrt{294}+12)}{150} = \frac{\sqrt{294}+12}{25} = 1 + \frac{\sqrt{294}-13}{25},\ u_4 = 1$
$\frac{25}{\sqrt{294}-13} = \frac{25(\sqrt{294}+13)}{125} = \frac{\sqrt{294}+13}{5} = 6 + \frac{\sqrt{294}-17}{5},\ u_5 = 6$
$\frac{5}{\sqrt{294}-17} = \frac{5(\sqrt{294}+13)}{5} = \sqrt{294} + 17 = 34 + (\sqrt{294} - 17),\ u_6 = 34.$
Hence

$$\sqrt{294} = \left[17, \overline{6, 1, 4, 1, 6, 34}\right].$$

Thus, we have the following table :

n	0	1	2	3	4	5	6
u_n	17	6	1	4	1	6	34
p_n	17	103	120	583	703	4801	163937
q_n	1	6	7	34	41	280	8721
$p_n^2 - 294q_n^2$	5	25	-6	-19	5	1	

Then, from theorem 11, the fundamental unit of $\mathcal{O}_7 = \mathbb{Z} + \mathbb{Z}\left[7\sqrt{6}\right]$ is : $4801 + 280.7\sqrt{6}$.

It follows that from theorem 16 all the solutions of the Pell's equation

$$x^2 - 294y^2 = 1$$

are given by :

$$x + y\sqrt{294} = \pm(4801 + 280\sqrt{294})^n,\ n \in \mathbb{Z}.$$

Example 2. Take $d = 5$. Then $d \equiv 1 \pmod 4$ is square-free such that $\mathbb{Q}(\sqrt{5})$ is a quadratic field. To find the fundamental unit of the order $\mathcal{O}_3 = \mathbb{Z}+\mathbb{Z}\left[3\sqrt{5}\right]$ of the field $\mathbb{Q}(\sqrt{5})$, we begin by develop the number $3\frac{\sqrt{5}-1}{2} = \frac{\sqrt{45}-3}{2}$ in continued fraction. We have :
$\frac{\sqrt{45}-3}{2} = 1 + \frac{\sqrt{45}-5}{2},\ u_0 = 1$
$\frac{2}{\sqrt{45}-5} = \frac{2(\sqrt{45}+5)}{20} = \frac{\sqrt{45}+5}{10} = 1 + \frac{\sqrt{45}-5}{10},\ u_1 = 1$
$\frac{10}{\sqrt{45}-5} = \frac{10(\sqrt{45}+5)}{20} = \frac{\sqrt{45}+5}{2} = 5 + \frac{\sqrt{45}-5}{2},\ u_2 = 1.$
Hence

$$\frac{\sqrt{45} - 3}{2} = \left[1, \overline{1, 5}\right].$$

Thus, we have the following table :

n	0	1	2
u_n	1	1	5
p_n	1	2	11
q_n	1	1	6
$4p_n^2 + 12p_nq_n - 36q_n^2$	-20	4	

Then, from theorem 11, the fundamental unit of $\mathcal{O}_3$ is : $\frac{7+3\sqrt{5}}{2}$.
It follows that from theorem 19 all the solutions of the Pell's equation

$$x^2 - 45y^2 = 4$$

are given by :

$$\frac{x + y\sqrt{45}}{2} = \pm \left(\frac{7 + 3\sqrt{5}}{2} \right)^n , \quad n \in \mathbb{Z}.$$

Example 3. To illustrate the use of remark 21 (or remark 18), take $d = 37$. Then $d \equiv 1 \pmod 4$ is square-free such that $\mathbb{Q}(\sqrt{37})$ is a quadratic field. To find the fundamental unit of the order $\mathcal{O}_1 = \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left[\sqrt{37}\right]$ of $\mathbb{Q}(\sqrt{37})$, we first develop the number $\frac{\sqrt{37}-1}{2}$ in continued fraction. We have

$\frac{\sqrt{37}-1}{2} = 2 + \frac{\sqrt{37}-5}{2}$, $u_0 = 2$
$\frac{2}{\sqrt{37}-5} = \frac{2(\sqrt{37}+5)}{12} = \frac{\sqrt{37}+5}{6} = 1 + \frac{\sqrt{37}-1}{6}$, $u_1 = 1$
$\frac{6}{\sqrt{37}-1} = \frac{6(\sqrt{37}+1)}{36} = \frac{\sqrt{37}+1}{6} = 1 + \frac{\sqrt{37}-5}{6}$, $u_2 = 1$
$\frac{6}{\sqrt{37}-5} = \frac{6(\sqrt{37}+5)}{12} = \frac{\sqrt{37}+5}{2} = 5 + \frac{\sqrt{37}-5}{2}$, $u_3 = 5$.
Hence

$$\frac{\sqrt{37} - 1}{2} = \left[2, \overline{1, 1, 5}\right] .$$

Next, we constituate the following table :

n	0	1	2	3
u_n	2	1	1	5
p_n	2	3	5	28
q_n	1	1	2	11
$4p_n^2 + 4p_nq_n - 36q_n^2$	-12	12	-4	

Then, the fundamental unit of $\mathcal{O}_1$ is : $\frac{12+2\sqrt{37}}{2}$.
According to remark 21, it follows that all the solutions of the equation

$$x^2 - 37y^2 = -4$$

are given by :

$$\frac{x + y\sqrt{37}}{2} = \pm \left(\frac{12 + 2\sqrt{37}}{2} \right)^{2n+1} , \quad n \in \mathbb{Z}.$$

References

[1] **L. Bapoungué**, *Un critère de résolution pour l'équation diophantienne* $ax^2 + 2bxy - kay^2 = \pm 1$. Expo. Math. Vol. 16, 3 (1998), p. 249-262.

[2] **L. Bapoungué**, *L'équation de Pell* $v^2 - (ka^2 + b^2)w^2 = -k$ *par les idéaux des corps quadratiques* $\mathbb{Q}(\sqrt{ka^2 + b^2})$. Expo. Math. 19 (2001), p. 251 - 266.

[3] **L. Bapoungué**, *On a special case of the Diophantine equation* $ax^2 + bx + c = dy^n$. Sciencia Acta Xaveriana. Vol. 2, n° 1, March 2011, p. 59-71.

[4] **Z. I. Borevitch et Chafarevitch**, *Théorie des nombres.* Gauthier-Villars, Paris, 1967.

[5] **J. P. Colette**, *Histoire des mathématiques.* Éditions du renouveau pédagogique Inc., Vol. 1, Ottawa, Canada, 1973.

[6] **P. Dubreuil et M. L. Dubreuil-Jacotin**, *Leçons d'algèbre moderne.* Dunod, Paris, 1961.

[7] **J. Itard**, *Arithmétique et Théorie des nombres.* Que sais-je ? PUF, Paris, 1973.

[8] **P. Kaplan**, *Pell's equations* $X^2 - mY^2 = -1, -4$ *and continued fractions.* J. Number Theory. Vol. 23, n° 2, June 1986.

[9] **C. D. Olds**, *Continued fractions.* The L. W. Singer Company, 1963.

[10] **A. Schinzel**, *On some problems of the arithmetical theory of continued fractions.* Acta Artith. 6 (1961), p. 394-413.

[11] **A. Schinzel**, *On some problems of the arithmetical theory of continued fractions.* Acta Artith. 7 (1962), p. 288-298.