International Journal of Pure and Applied Mathematics
Volume 64 No. 2 2010, 305-316

GENERALIZED REDÉI RATIONAL FUNCTIONS AND RATIONAL APPROXIMATIONS OVER CONICS

Stefano Barbero[1], Umberto Cerruti[2] §, Nadir Murru[3]
[1,2,3]Department of Mathematics
University of Turin
10, Via Carlo Alberto, Turin, 10123, ITALY
[1]e-mail: stefano.barbero@unito.it
[2]e-mail: umberto.cerruti@unito.it
[3]e-mail: nadir.murru@unito.it

Abstract: In this paper we study a general class of conics starting from a quotient field. We give a group structure over these conics generalizing the construction of a group over the Pell hyperbola. Furthermore, we generalize the definition of Redéi rational functions in order to use them for evaluating powers of points over these conics. Finally, we study rational approximations of irrational numbers over conics, obtaining a new result for the approximation of quadratic irrationalities.

AMS Subject Classification: 11B39, 11D09, 11J68
Key Words: continued fractions, groups over conics, quadratic irrationalities, rational approximations, Redéi rational functions

1. Introduction

In a previous paper [1] we defined an operation over $\mathbb{R}^\infty = \mathbb{R} \cup \{\infty\}$, which allowed us to construct a group over the Pell hyperbola

$$H_d = \{(x, y) \in \mathbb{R}^2 : x^2 - dy^2 = 1\}.$$

In this paper we want to work on a more general class of conics

$$E_{\mathbb{F}}(h, d) = \{(x, y) \in \mathbb{F}^2 : x^2 + hxy - dy^2 = 1\}$$

over an ordinary field $\mathbb{F}$. In this case the conics are not only hyperbolae, but

Received: August 12, 2010
§Correspondence author

they can be ellipses or parabolae, depending on the quantity h^2+4d to be positive, negative or zero respectively. Here we study some properties of such conics and, in particular, we will see how to construct a group over them, generalizing the classic construction over the Pell hyperbola. Furthermore, in [1] we showed how Redéi rational functions (see [6]) can be used over the Pell hyperbola in order to find solutions of the Pell equation in a new way. Redéi rational functions are very interesting and useful in number theory, finding many applications, e.g., in the permutations of finite field, in cryptography (for these applications and a good theory about Redéi rational functions see [4]) or in pseudorandom sequences (see [7]). Here we obtain some polynomials which generalize the Redéi rational functions and which are usable over the conics $E_{\mathbb{F}}(h,d)$ in order to evaluate powers of points. Finally, considering $\mathbb{F}=\mathbb{R}$, we study approximations of irrational numbers through sequences of rational numbers which lie over conics.

First of all we see how we can obtain the conics $E_{\mathbb{F}}(h,d)$ starting from a simple quotient field.

Definition 1. Let $\mathbb{F}$ be a field and x^2-hx-d an irreducible polynomial over $\mathbb{F}[x]$. We consider the quotient field

$$\mathbb{A}=\mathbb{F}[x]/(x^2-hx-d)\ .$$

For any two elements $a+bx, u+vx\in\mathbb{A}$, the product naturally induced is

$$(a+bx)(u+vx)=(au+bvd)+(bu+av+bvh)x\ ,$$

while the norm, the trace and the conjugate of an element $a+bx\in\mathbb{A}$, respectively, are well defined as follows:

$N(a+bx)=a^2+hab-db^2$, $\quad Tr(a+bx)=2a+hb$, $\quad \overline{a+bx}=(a+hb)-bx$.

Indeed

$$(a+bx)(\overline{a+bx})=N(a+bx)\ .$$

Consequently the inverse of an element in $\mathbb{A}$ is

$$(a+bx)^{-1}=\frac{\overline{a+bx}}{N(a+bx)}\ .$$

Now we consider the group of the unitary elements of $\mathbb{A}^*=\mathbb{A}-\{0\}$

$$U=\{a+bx\in\mathbb{A}^* : N(a+bx)=1\}=\{a+bx\in\mathbb{A}^* : a^2+hab-db^2=1\}\ .$$

So we have a natural bijection between U and the set of points

$$E=E_{\mathbb{F}}(h,d)=\{(x,y)\in\mathbb{F} : x^2+hxy-dy^2=1\}\ ,$$

which induces the commutative product $\odot_E$ over E

$$(x,y)\odot_E(u,v)=(xu+yvd, yu+xv+yvh)\ ,\quad \forall (x,y),(u,v)\in E\ .$$

We immediately have the following

Proposition 2. *$(E, \odot_E)$ is an Abelian group with identity $(1,0)$ and the inverse of an element $(x,y) \in E$ is*

$$(x,y)^{-1} = (x + hy, -y).$$

We can parametrically represent the conics E using

$$y = \frac{1}{m}(x+1). \tag{1}$$

Considering $P = \mathbb{F} \cup \{\alpha\}$, where with α we indicate an element not in $\mathbb{F}$, we directly find the bijections

$$\begin{cases} \epsilon : P \to E, \\ \epsilon : m \mapsto \left(\dfrac{m^2+d}{m^2+hm-d}, \dfrac{2m+h}{m^2+hm-d} \right), \quad \forall m \in \mathbb{F}, \\ \epsilon(\alpha) = (1,0)\ , \end{cases} \tag{2}$$

and

$$\begin{cases} \tau : E \to P, \\ \tau : (x,y) \mapsto \dfrac{1+x}{y}, \quad \forall (x,y) \in E, \quad y \neq 0, \\ \tau(1,0) = \alpha, \\ \tau(-1,0) = -\dfrac{h}{2}\ , \end{cases}$$

i.e. P is a parametric representation of E. Now, using ϵ and τ, we can naturally induce a commutative product $\odot_P$ over the representation P

$$\tau(s,t) \odot_P \tau(u,v) = \epsilon^{-1}((x,y) \odot_E (u,v)), \quad \forall (s,t),(u,v) \in E.$$

In particular, α becomes the identity with respect to $\odot_P$ and

$$a \odot_P b = \frac{d+ab}{h+a+b}, \quad \forall a,b \in P\ ,\ a+b \neq -h\ . \tag{3}$$

If $a+b=-h$, we set $a \odot_P b = \alpha$, so a corresponds to the inverse of b over $(P, \odot_P)$, and clearly

Proposition 3. *$(P, \odot_P)$ is an Abelian group.*

Remark 4. Let us consider the quotient group $B = \mathbb{A}^*/\mathbb{F}^*$, whose elements

$$[a+bx] = \{\lambda a + \lambda b x : \lambda \in \mathbb{F}^*\}\ ,$$

correspond to the equivalence class of $a + bx \in \mathbb{A}^*$. Of course if $b = 0$, then

$[a+bx]=[a]=[1_{\mathbb{F}^*}]$, and

$$B=\{[a+x]:a\in\mathbb{F}\}\cup\{[1_{\mathbb{F}^*}]\}\ .$$

The product in B is given by

$$[a+x][b+x]=[ab+ax+bx+x^2]=[(d+ab)+(h+a+b)x]\ ,$$

and, if $h+a+b\neq 0$, then

$$[a+x][b+x]=[\frac{d+ab}{h+a+b}+x]\ ,$$

else

$$[a+x][b+x]=[d+ab]=[1_{\mathbb{F}^*}].$$

But comparing this with the product (3) we find an immediate isomorphism

$$\begin{cases}\phi:B\to P,\\ \phi:[a+x]\mapsto a,\quad [a+x]\neq[1_{\mathbb{F}^*}],\\ \phi([1_{\mathbb{F}^*}])=\alpha,\end{cases}$$

which shows how $\odot_P$ can be induced in an alternative way, starting from the quotient group B.

2. Generalized Redéi Rational Functions

The aim of this section is to show how Redéi rational functions can be generalized and how they are strictly related with the product $\odot_P$. Let us recall that the n-th power of the matrix

$$M=\begin{pmatrix}z+h & d\\ 1 & z\end{pmatrix},\quad h,d,z\in\mathbb{F}\ , \tag{4}$$

can be determined employing two kinds of polynomials, $N_n=N_n(h,d,z)$ and $D_n=D_n(h,d,z)$, obtaining

$$M^n=\begin{pmatrix}N_n+hD_n & dD_n\\ D_n & N_n\end{pmatrix}\ .$$

A direct calculation and an easy inductive proof can show that N_n and D_n are the terms of two linear recurrent sequences, as we point out in the next

Remark 5. If we indicate with $\mathcal{W}(a,b,r,k)$ the linear recurrent sequence over $\mathbb{F}$, with initial conditions a,b and characteristic polynomial t^2-rt+k, then

$$N_n(h,d,z)=\mathcal{W}(1,z,2z+h,z^2+hz-d),$$

$$D_n(h,d,z) = \mathcal{W}(0,1,2z+h,z^2+hz-d).$$

Moreover, in the following proposition we emphasize two important relations involving N_n and D_n

Proposition 6.

$$\begin{cases} N_{n+m} = N_nN_m + dD_nD_m, \\ D_{n+m} = D_nN_m + hD_nD_m + N_nD_m. \end{cases}$$

Proof. The proof is straightforward and only consists in comparing the resulting matrix on the right with the one on the left of the equality

$$\begin{pmatrix} N_{n+m}+hD_{n+m} & dD_{n+m} \\ D_{n+m} & N_{n+m} \end{pmatrix} = \begin{pmatrix} N_n+hD_n & dD_n \\ D_n & N_n \end{pmatrix}\begin{pmatrix} N_m+hD_m & dD_m \\ D_m & N_m \end{pmatrix}. \quad \square$$

We observe that

$$\det(M^n) = [\det(M)]^n = (z^2+hz-d)^n \ ,$$

on the other hand

$$\det(M^n) = N_n^2 - hN_nD_n - dD_n^2 = (z^2+hz-d)^n,$$

so, when $z^2+hz-d=1$, all points (N_n,D_n) lie on $E_{\mathbb{F}}(h,d)$.

Finally, we can define the *generalized Redéi rational functions*

$$Q_n(h,d,z) = \frac{N_n(h,d,z)}{D_n(h,d,z)}, \quad \forall n \geq 1 \ . \tag{5}$$

Obviously, when $\mathbb{F}=\mathbb{R}$ and $h=0$, $Q_n(h,d,z) = Q_n(d,z)$, and we find the usual Redéi rational functions. The $Q_n(h,d,z)$ have an interesting behaviour with respect to $\odot_P$, which reveals some important aspects of these functions, in particular they can be viewed as a kind of powers. These facts are summarized in the following proposition and remarks.

Proposition 7. *For any $h,d,z \in \mathbb{F}$*

$$Q_{n+m}(h,d,z) = Q_n(h,d,z) \odot_P Q_m(h,d,z) \ .$$

Proof. Using Proposition 6 we have

$$\frac{N_n}{D_n} \odot_P \frac{N_m}{D_m} = \frac{d+\frac{N_n}{D_n}\frac{N_m}{D_m}}{h+\frac{N_n}{D_n}+\frac{N_m}{D_m}} = \frac{dD_nD_m+N_nN_m}{hD_nD_m+D_mN_m+D_nN_m} = \frac{N_{n+m}}{D_{n+m}}. \quad \square$$

Remark 8. Since

$$Q_1(h,d,z) = z,$$

then

$$Q_n(h,d,z) = z^{n_{\odot_P}} = \underbrace{z \odot_P \ldots \odot_P z}_{n-times} ,$$

i.e., the functions Q_n are intimately related to $\odot_P$, essentially being powers under this product, and the multiplicative property clearly holds for these functions

$$Q_n(h,d,Q_m(h,d,z)) = (Q_m(h,d,z))^{n_{\odot_P}} = (z^{m_{\odot_P}})^{n_{\odot_P}} = z^{nm_{\odot_P}} = Q_{nm}(h,d,z).$$

Remark 9. If we set $Q = \{Q_n(h,d,z), \forall n\}$, then $(Q, \odot_P, \circ)$, where $\circ$ is the usual composition between functions, is a commutative ring isomorphic to $(\mathbb{Z}, +, \cdot)$ and

$$Q_n(h,d,\cdot) : (P, \odot_P) \to (P, \odot_P), \quad \forall n \geq 1 ,$$

are morphisms, since $Q_n(h,d,z) = z^{n_{\odot_P}}$.

3. Evaluating Powers of Points

What we have showed in the previous section allows us to focus the attention on points of E and especially on their powers. We are ready to explain how powers of points belonging to E can be evaluated, using the generalized Redéi rational functions $Q_n(h,d,z)$.

Let (x,y) be a point of E, setting $(x_n,y_n) = (x,y)^{n_{\odot_E}}$, an inductive arguments and a little bit of calculation can be easily used to prove that

$$\begin{cases} x_n = \mathcal{W}(1,x,2x+hy,1) = F_n(h,x,y) = F_n, \\ y_n = \mathcal{W}(0,y,2x+hy,1) = G_n(h,x,y) = G_n \ . \end{cases} \tag{6}$$

Now, finding what is the image of $(x,y)^{n_{\odot_E}}$ under τ, we have the equalities

$$\tau((x,y)^{n_{\odot_E}}) = \left(\frac{1+x}{y}\right)^{n_{\odot_P}} = Q_n\left(h,d,\frac{1+x}{y}\right) ,$$

and

$$\tau((x,y)^{n_{\odot_E}}) = \tau(x_n,y_n) = \tau(F_n,G_n) = \frac{1+F_n}{G_n} .$$

Furthermore, recalling that we are working with points (x,y) of E, satisfying

$x^2 + hxy - dy^2 = 1$, we can eliminate the dependence from d

$$q_n(h,x,y) = Q_n\left(h, \frac{1-hxy-x^2}{y^2}, \frac{1+x}{y}\right) = \frac{1+F_n(h,x,y)}{G_n(h,x,y)} .$$

Finally, by Remark 5 and (6) we have

$$q_n(h,x,y) = \frac{1+N_n(hy, x^2+hxy-1, x)}{yD_n(hy, x^2+hxy-1, x)} . \tag{7}$$

From the last equality (7) we discover another interesting relation, proved in the following

Proposition 10. *Given $(x,y) \in E_{\mathbb{F}}(h,d)$, then*

$$q_{2n}(h,x,y) = \frac{F_n(h,x,y)}{G_n(h,x,y)} .$$

Proof. For the sake of simplicity, here we write N_n and D_n instead of $N_n(hy, x^2+hxy-1, x)$, $D_n(hy, x^2+hxy-1, x)$. By (7), we have to show

$$\frac{1+N_{2n}}{yD_{2n}} = \frac{N_n}{yD_n} .$$

So we consider

$$\frac{1+N_{2n}}{D_{2n}} - \frac{N_n}{D_n} = \frac{D_n + D_nN_{2n} - N_nD_{2n}}{D_{2n}D_n} .$$

Clear consequences of Proposition 6 are the relations

$$\begin{cases} N_{2n} = N_n^2 + dD_n^2, \\ D_{2n} = 2N_nD_n + hyD_n^2 , \end{cases}$$

where in this case $d = x^2 + hxy - 1$. Now we can easily evaluate the quantity $D_n + D_2N_{2n} - N_nD_{2n}$, finding

$$\begin{aligned} D_n + D_2N_{2n} - N_nD_{2n} &= D_n + D_n(N_n^2 + dD_n^2) - N_n(2N_nD_n + hyD_n^2) \\ &= D_n(1 - N_n^2 + dD_n^2 - hyN_nD_n) = D_n(1 - \det(M^n)) = 0, \end{aligned}$$

since $\det(M^n) = x^2 + hxy - d = x^2 + hxy - x^2 - hxy + 1 = 1$, and M is the matrix defined in (4). □

4. Approximations over Conics

An interesting research field involves the study of approximations of irrational numbers by sequences of rationals, which can be viewed as sequences of points

over conics. In [2] it has been proved that if a conic has a rational point, then there are irrational numbers β such that there exists an infinite sequence of nonzero integer triples (x_n, y_n, z_n), where $\frac{x_n}{y_n}$ are rational approximations of β and $\left(\frac{x_n}{z_n}, \frac{y_n}{z_n}\right)$ are rational points of the conic. Another interesting result has been proved in [3], where rational approximations via Pythagorean triples has been studied, considering rational approximations $\frac{x}{y}$ of β when $x^2 + y^2$ is a perfect square. The common point of these results is that auxiliary irrationals, depending on β, have been used and these auxiliary irrationals must have a continued fraction expansion with unbounded partial quotients (see Lemma 7 in [2] and Theorem 1.1 in [3]). In this way, it is not possible to approximate, for example, quadratic irrationalities. Here, using powers of points studied in the previous section, we will see that we can approximate quadratic irrationalities and we do not have the problem of unbounded partial quotients.

In this section we will always consider $\mathbb{F} = \mathbb{R}$. First of all, we need the following

Lemma 11. *Let*

$(a_n)_{n=0}^{+\infty} = \mathcal{W}(a_0, a_1, 2w, w^2 - c)$ *and* $(b_n)_{n=0}^{+\infty} = \mathcal{W}(b_0, b_1, 2w, w^2 - c)$

be rational sequences, we have

$$\lim_{n\to+\infty} \frac{a_n}{b_n} = \frac{a_1 - a_0 w + a_0\sqrt{c}}{b_1 - b_0 w + b_0\sqrt{c}}\,.$$

Proof. For the Binet formula

$$a_n = A_1(w + \sqrt{c})^n + A_2(w - \sqrt{c})^n \quad \text{and} \quad b_n = B_1(w + \sqrt{c})^n + B_2(w - \sqrt{c})^n\,,$$

for every $n \geq 0$ and $A_1, A_2, B_1, B_2 \in \mathbb{C}$. So

$$\lim_{n\to+\infty} \frac{a_n}{b_n} = \lim_{n\to+\infty} \frac{A_1(w + \sqrt{c})^n + A_2(w - \sqrt{c})^n}{B_1(w + \sqrt{c})^n + B_2(w - \sqrt{c})^n} = \frac{A_1}{B_1}\,.$$

We can find A_1, B_1 simply solving the systems

$$\begin{cases} A_1 + A_2 = a_0, \\ A_1(x + \sqrt{c}) + A_2(x - \sqrt{c}) = a_1, \end{cases} \quad \text{and} \quad \begin{cases} B_1 + B_2 = b_0, \\ B_1(x + \sqrt{c}) + B_2(x - \sqrt{c}) = b_1. \end{cases}$$

We obtain the values

$$A_1 = -\frac{a_1 - a_0(x - \sqrt{c})}{2\sqrt{c}} \quad \text{and} \quad B_1 = -\frac{b_1 - b_0(x - \sqrt{c})}{2\sqrt{c}}\,,$$

from which the thesis easily follows. □

Now we can see that powers of points, which obviously lie over the conic from Proposition 2, converge to a quadratic irrationality.

Theorem 12. *Given a rational point $(x,y) \in E$ and $(x_n, y_n) = (x,y)^{n\odot_E}$, we have*

$$\lim_{n\to\infty} \frac{y_n}{x_n} = \frac{2y}{\sqrt{h^2y^2 + 4hxy + 4x^2 - 4} - hy}.$$

Proof. As we have seen in the previous section

$$(x_n)_{n=0}^{+\infty} = \mathcal{W}(1, x, 2x + hy, 1), \quad (y_n)_{n=0}^{+\infty} = \mathcal{W}(0, y, 2x + hy, 1) \ .$$

Here we will use the Lemma 11, where the initial conditions are

$$x_0 = 0, \quad x_1 = y, \quad y_0 = 1, \quad y_1 = x \ ,$$

and we have the equalities

$$2w = 2x + hy, \quad w^2 - c = 1 \ ,$$

which give

$$w = \frac{2x + hy}{2} \ , \quad c = \frac{h^2y^2 + 4hxy + 4x^2 - 4}{4} \ .$$

Thus, by the Lemma 11,

$$\lim_{n\to\infty} \frac{y_n}{x_n} = \frac{a_1 - a_0w + a_0\sqrt{c}}{b_1 - b_0w + b_0\sqrt{c}} = \frac{2y}{\sqrt{h^2y^2 + 4hxy + 4x^2 - 4} - hy}. \qquad \square$$

Example 13. Let us consider the conic $E = E_{\mathbb{R}}(-13/4, 2)$ and the rational point $(4,1)$ over this conic. The powers of this point with respect to $\odot_E$ are

$$\left(18, \frac{19}{4}\right), \left(\frac{163}{2}, \frac{345}{16}\right), \left(\frac{2953}{8}, \frac{6251}{64}\right), \left(\frac{53499}{32}, \frac{113249}{256}\right), \dots \ .$$

From the last Theorem 12, we know that

$$\left(\frac{1}{4}, \frac{19}{72}, \frac{345}{1304}, \frac{6251}{23624}, \frac{113249}{427992}, \dots\right)$$
$$= (0.25, 0.26388, 0.26457, 0.26460, 0.26460, \dots)$$

are rational approximations of a quadratic irrationality, which in this case is

$$\frac{8}{13 + 3\sqrt{33}} \cong 0.264605 \dots \ .$$

Furthermore, we can see how it is easy to construct rational approximations for every irrational number such that these approximations form points over conics. Let us consider a conic C with a rational parametrization, i.e.,

$$\begin{cases} x = f(m), \\ y = g(m) \ , \end{cases}$$

for any point $(x, y) \in C$ and f, g rational functions. If we take any irrational number β, we are able to construct rational approximations $\frac{x_n}{y_n}$ of β such that $(x_n, y_n) \in C$. Indeed, we have only to find the irrational number α such that

$$\frac{g(\alpha)}{f(\alpha)} = \beta \tag{8}$$

and then to consider the continued fraction expansion of α. We recall that a continued fraction is a representation of a real number α through a sequence of integers as follows:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

where the integers $a_0, a_1, ...$ can be evaluated with the recurrence relations

$$\begin{cases} a_k = [\alpha_k] \\ \alpha_{k+1} = \dfrac{1}{\alpha_k - a_k} \quad \text{if } \alpha_k \text{ is not an integer} \end{cases} \qquad k = 0, 1, 2, ...$$

for $\alpha_0 = \alpha$ (see [5]). A continued fraction can be expressed in a compact way using the notation $[a_0, a_1, a_2, a_3, ...]$. The finite continued fraction

$$[a_0, ..., a_n] = \frac{p_n}{q_n}, \quad n = 0, 1, 2, ... \tag{9}$$

is a rational number and is called the n–th *convergent* of $[a_0, a_1, a_2, a_3, ...]$. Now, if we consider the sequences $(p_n)_{n=0}^{+\infty}$ and $(q_n)_{n=0}^{+\infty}$, coming from (9), the sequences $(x_n)_{n=0}^{+\infty}$ and $(y_n)_{n=0}^{+\infty}$ have general terms

$$x_n = f\left(\frac{p_n}{q_n}\right), \quad y_n = g\left(\frac{p_n}{q_n}\right), \quad n = 0, 1, 2, \dots , \tag{10}$$

which satisfy

$$\lim_{n\to\infty} \frac{y_n}{x_n} = \lim_{n\to\infty} \frac{g(\frac{p_n}{q_n})}{f(\frac{p_n}{q_n})} = \frac{g(\alpha)}{f(\alpha)} = \beta$$

and clearly $(x_n, y_n) \in C$, $\forall n \geq 0$. The only conditions that we require are that equation (8) has irrational solutions and the conic C has a rational point (and in this case it means that it has infinite rational points). In the case of our conics $E = E_{\mathbb{R}}(h, d)$ we have no problems. Indeed, $(-1, 0), (1, 0) \in E$ and any

point $(x, y) \in E$, has a parametric representation (2)

$$\begin{cases} x = f(m) = \dfrac{m^2 + d}{m^2 + hm - d}, \\ y = g(m) = \dfrac{2m + h}{m^2 + hm - d} \, . \end{cases}$$

In this case equation (8) becomes

$$\frac{2\alpha + h}{\alpha^2 + d} = \beta \ ,$$

which has solutions

$$\alpha = \frac{1 \pm \sqrt{1 + \beta^2}}{\beta}.$$

and α is always an irrational number.

Finally, we consider the interesting case given by $h = 0, d = -1$, i.e., the conic

$$E = E_{\mathbb{R}}(0, 1) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

is the unitary circle. In this case we can construct infinite rational approximations by Pithagorean triples. Indeed, in this case equations (10) give

$$x_n = \frac{p_n^2 - q_n^2}{p_n^2 + q_n^2}, \quad y_n = \frac{2p_n q_n}{p_n^2 + q_n^2}, \quad n = 0, 1, 2, \dots \ ,$$

and

$$\lim_{n \to \infty} \frac{y_n}{x_n} = \lim_{n \to \infty} \frac{2p_n q_n}{p_n^2 - q_n^2} = \beta \ . \tag{11}$$

Since $(x_n, y_n) \in E$, $\forall n \geq 0$, we trivially have

$$(p_n^2 - q_n^2)^2 + (2p_n q_n)^2 = (p_n^2 + q_n^2)^2.$$

We conclude this paper with an example of the approximation of π over the circle.

Example 14. Let us consider $\beta = \pi$ the irrational number that we want to approximate over E. We use as auxiliary irrational

$$\alpha = \frac{1 + \sqrt{1 + \pi^2}}{\pi} \ ,$$

which has the continued fraction expansion

$$\alpha = [1, 2, 1, 2, 1, 1, 3, 1, 1, 5, \dots] \ .$$

The sequences $(p_n), (q_n)$ which determine the convergents are

$$(1, 3, 4, 11, 15, 26, 93, 119, 212, 1179, \dots)$$

$$(1, 2, 3, 8, 11, 19, 68, 87, 155, 862, \ldots) .$$

By (11) the approximations of π are

$$\left(\frac{12}{5}, \frac{24}{7}, \frac{176}{57}, \frac{165}{52}, \frac{988}{315}, \frac{12648}{4025}, \frac{10353}{3296}, \frac{65720}{20919}, \frac{2032596}{646997}, \ldots\right) ,$$

indeed they are

$$(2.4, 3.4285, 3.0877, 3.1730, 3.1365, 3.1423, 3.1410, 3.1416, 3.1415, \ldots).$$

Furthermore, the points

$$\left(\frac{5}{13}, \frac{12}{13}\right), \left(\frac{7}{25}, \frac{24}{25}\right), \left(\frac{57}{185}, \frac{176}{185}\right), \left(\frac{52}{346}, \frac{165}{346}\right), \left(\frac{315}{1037}, \frac{988}{1037}\right), \ldots$$

lie on the circle and thus we have the following Pythagorean triples

$$(5, 12, 13), (7, 24, 25), (57, 176, 185), (52, 165, 346), (315, 988, 1037), \ldots .$$

References

[1] S. Barbero, U. Cerruti, N. Murru, Solving the Pell equation via Redéi rational functions, *The Fibonacci Quarterly* (2010), Accepted.

[2] E.B. Burger, A.M. Pillai, On Diophantine approximation along algebraic curves, *Proceedings of the American Mathematical Society*, **136**, No. **1** (2008), 11-19.

[3] C. Elsner, On rational approximations by Pythagorean numbers, *The Fibonacci Quarterly*, **42**, No. 2 (2003), 98-104.

[4] R. Lidl, G.L. Mullen, *Dickson Polynomials*, Pitman Monogr., Surveys Pure Appl. Math., **65**, Longman (1993).

[5] C.D. Olds, *Continued Fractions*, Random House (1963).

[6] L. Rédei, Über eindeuting umkehrbare Polynome in endlichen Korpen, *Acta Sci. Math.*, Szeged, **11** (1946), 85-92.

[7] A. Topuzoglu, A. Winterhof, Topics in geometry, coding theory and cryptography, *Algebra and Applications*, **6** (2006), 135-166.