Rational approximations over conics

Stefano Barbero

Introduction

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

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

For a couple of elements $a + bx, u + vx \in \mathbb{A}$, the natural product defined on $\mathbb{A}$ is

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

and it is straightforward to observe that the norm of an element is $N(a + bx) = a^2 + hab - db^2$. In this way we find an one to one correspondence between the set of unitary elements belonging to $\mathbb{A}$ and set of points

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

Remark

When $\mathbb{F} = \mathbb{R}$, $E_{\mathbb{F}}(h, d)$ represents a non–degenerate conic, of hyperbolic, elliptic or parabolic type if $h^2 + 4d$ is positive, negative or equal to 0, respectively.

Remark

The natural product defined on $\mathbb{A}$ induces the product $\odot_E$ on E:

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

Proposition

$(E, \odot_E)$ is an abelian group with the identity corresponding to the point $(1, 0)$ and the inverse of an element $(x, y) \in E$ given by

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

Main results

Let us consider $P = \mathbb{F} \cup \{\alpha\}$, where α is an element not belonging to $\mathbb{F}$. We can directly find the following bijections

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

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.

Using ϵ and τ, we can induce a commutative product $\odot_P$ over 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 the product $\odot_P$ and

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

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

Proposition

$(P, \odot_P)$ *is an abelian group.*

Now we give a generalization of Rédei rational functions in such a way that these new functions will show a "good" behaviour in relation with the product $\odot_P$. Starting from the matrix

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

we introduce the polynomials $N_n = N_n(h, d, z)$, $D_n = D_n(h, d, z)$ satisfying the relation

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

We define the generalized Rédei rational functions as

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

Proposition

For all $h, d, z \in \mathbb{F}$ *and* n, m *natural numbers with* $n, m \geq 1$

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

Remark

Since we have $Q_1(h,d,z) = z$, *then*

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

Proposition

The following multiplicative property holds

$$Q_n(h,d,Q_m(h,d,z)) = (Q_m(h,d,z))^{n_{\odot_P}}$$

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

With analogous considerations like the ones related to the Rédei rational functions over the Pell hyperbola, these new rational functions could be used to calculate powers of points over our conics with respect to the product $\odot_E$.

Proposition

Let (x,y) a point belonging to E, if we consider $(x,y)^{n_{\odot_E}} = (x_n, y_n)$, then $Q_{2n}\left(h, \frac{1-hxy-x^2}{y^2}, \frac{1+x}{y}\right) = \frac{x_n}{y_n}.$

Applications

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 the paper of Burger and Pillai 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 $\frac{y_n}{x_n}$ 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 the paper of Elsner, 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.

Remark

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 Burger and Pillai and Theorem 1.1 in the paper of Elsner). In this way, it is not possible to approximate, for example, quadratic irrationalities. Here, using powers of points previously introduced, we can approximate quadratic irrationalities and we do not have the problem of unbounded partial quotients.

When $\mathbb{F} = \mathbb{R}$, powers of points which lie over the conic $E_{\mathbb{R}}(h, d)$ converge to a quadratic irrationality.

Theorem

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

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

Example

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*

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

From the last Theorem, we know that

$$\left(\frac{1}{4}, \frac{19}{72}, \frac{345}{1304}, \frac{6251}{23624}, \frac{113249}{427992}, \ldots\right)$$

are rational approximations of a quadratic irrationality, which in this case is $\dfrac{8}{13 + 3\sqrt{33}} \cong 0.264605\ldots$.

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 $\frac{y_n}{x_n}$ of β such that $(x_n, y_n) \in C$. We have only to find the irrational number α such that

$$\frac{g(\alpha)}{f(\alpha)} = \beta \quad (1)$$

and then to consider the continued fraction expansion of α.

Definition

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 $a_0, a_1, \ldots$ *can be evaluated with the following recurrence relations, where* $[\alpha]$ *denotes the integer part of* α *and* $\alpha_0 = \alpha$ *(see, e. g., the book of Olds)*

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

Remark

A continued fraction can be expressed in a compact way using the notation $[a_0, a_1, a_2, a_3, ...]$, *where the finite continued fraction*

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

is a rational number and is called the n–th convergent of $[a_0, a_1, a_2, a_3, ...]$.

The sequences (x_n), (y_n) have general terms

$x_n = f\left(\frac{p_n}{q_n}\right), \quad y_n = g\left(\frac{p_n}{q_n}\right) \quad n = 0, 1, 2, \ldots$, which satisfy

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

Remark

Clearly $(x_n, y_n) \in C$, $\forall n \geq 0$, the only conditions that we require are that equation (1) has irrational solutions and the conic C has a rational point. 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

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

In this case equation (1) becomes $\dfrac{2\alpha + h}{\alpha^2 + d} = \beta$, which has solutions $\alpha = \dfrac{1 \pm \sqrt{1 + \beta h - d\beta^2}}{\beta}$ and α is always an irrational number.

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 the parametric representations of E give

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

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

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

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

Example

We give an approximation over the unitary circle E of $\beta = \pi$ *by means of Pythagorean triples.*

We consider $\alpha = \dfrac{1 + \sqrt{1 + \pi^2}}{\pi}$ *, which has the continued fraction expansion* $\alpha = [1, 2, 1, 2, 1, 1, 3, 1, 1, 5, \ldots]$.

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

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

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

Example

By (2) the approximations of π are

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

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

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

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

Bibliography

- S. Barbero, U. Cerruti, N. Murru, Solving the Pell equation via Rédei rational functions, Accepted for publication in *The Fibonacci Quarterly*, (2010).
- E. B. Burger, A. M. Pillai, On diophantine approximation along algebraic curves, *Proceedings of the American Mathematical Society*, Vol. **136** No. **1** (2008), 11–19.
- C. Elsner, On rational approximations by Pythagorean numbers, *The Fibonacci Quarterly*, **42(2)** (2003,98–104.
- R. Lidl, G. L. Mullen, *Dickson polynomials*, Pitman Monogr., Surveys Pure appl. Math. **65**, Longman, (1993).
- C. D. Olds, *Continued fractions*, Random House, (1963).
- L. Rédei, Uber eindeuting umkehrbare polynome in endlichen korpen, *Acta Sci. Math.* (Szeged), **11** (1946), 85–92.
- A. Topuzoglu, A. Winterhof, Topics in geometry, coding theory and cryptography, *Algebra and Applications*, Vol. **6** (2006), 135–166.