A note on the use of Rédei polynomials for solving the polynomial Pell equation and its generalization to higher degrees

A note on the use of Rédei polynomials for solving the polynomial Pell equation and its generalization to higher degrees

Nadir Murru
Department of Mathematics G. Peano, University of Torino
Via Carlo Alberto 10, 10123, Torino, ITALY
nadir.murru@unito.it

Abstract

The polynomial Pell equation is

$$P^2 - DQ^2 = 1$$

where D is a given integer polynomial and the solutions P, Q must be integer polynomials. A classical paper of Nathanson [11] solved it when $D(x) = x^2 + d$. We show that the Rédei polynomials can be used in a very simple and direct way for providing these solutions. Moreover, this approach allows to find all the integer polynomial solutions when $D(x) = f^2(x) + d$, for any $f \in \mathbb{Z}[X]$ and $d \in \mathbb{Z}$, generalizing the result of Nathanson. We are also able to find solutions of some generalized polynomial Pell equations introducing an extension of Rédei polynomials to higher degrees.

Keywords: Pell equation, polynomial Pell equation, Rédei polynomial
2010 Mathematics Subject Classification: 11A99, 11D41, 11R09

1 Introduction

The Pell equation

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

is one of the most famous Diophantine equations. It has infinite integer solutions when d is not a square and they can be determined using the continued fraction's expansion of $\sqrt{d}$. It is very interesting to study the polynomial Pell equation, i.e., find polynomials P and Q in $\mathbb{Z}[X]$ satisfying

$$P^2 - DQ^2 = 1 \tag{1}$$

where $D \in \mathbb{Z}[X]$ is a fixed polynomial. Nathanson [11] solved the polynomial Pell equation when $D = x^2 + d$. In particular, he proved that it has non-trivial solutions if and only if $d = \pm 1, \pm 2$ and provided explicitly the polynomial solutions. Pastor [13] showed that the solutions of Nathanson can be also expressed in terms of Chebyshev polynomials. Webb and Yokota [17] found a necessary and sufficient condition for which the polynomial Pell equation has non-trivial solutions when $D = A^2 + 2C$ monic polynomial, $A/C \in \mathbb{Z}[X]$ and $\deg C < 2$. In [18], such result is generalized when $pA/C \in \mathbb{Z}[X]$, for some prime p, without any condition on the degree of C. In this case, the authors also determined the solutions. Then, Yokota [19] found a necessary and sufficient condition for the solution of the polynomial Pell equation when $A/C \in \mathbb{Q}[X]$. Hazama [7] studied the polynomial Pell equation using the twist of a conic by another conic. Further studies can be found in [10] and [14]. Mc Laughlin [9] focused on the relations between polynomial solutions of the Pell equation and fundamental units of real quadratic fields. Some authors studied polynomial solutions of (1) in $\mathbb{C}[X]$, see [4], [6], [20]. Despite many studies on the polynomial Pell equation, there are no works that highlight its connection with the Rédei polynomials, which are also classical tools in number theory, see [15], [8]. In this paper, we show this connection and how using Rédei polynomials for solving (1) for polynomials D more general than the polynomials studied in previous works.

The paper is structured as follows. We introduce the Rédei polynomials in section 2 where we show that solutions of (1) are the Rédei polynomials for some kind of polynomials D. The solutions

of Nathanson arise as particular cases. The used method, even if simple and straightforward, is very general and allows to approach also polynomial Pell equations with higher degrees by means of a generalization of the Rédei polynomials, as we will see in section 3.

2 Solution of the polynomial Pell equation via Rédei polynomials

Rédei polynomials were introduced in [15] and they are a particular case of Dickson polynomials [8]. They arise from the development of

$$(\sqrt{\alpha}+z)^n = D_n(\alpha,z)\sqrt{\alpha}+N_n(\alpha,z), \quad n=0,1,\dots$$

where $z,\alpha\in\mathbb{Z}$, α not square. They can be written in the following closed form:

$$N_n(\alpha,z)=\sum_{k=0}^{[n/2]}\binom{n}{2k}\alpha^k z^{n-2k}, \quad D_n(\alpha,z)=\sum_{k=0}^{[n/2]}\binom{n}{2k+1}\alpha^k z^{n-2k-1}.$$

It will be very useful the following matricial identity that can be easily proved by induction:

$$\begin{pmatrix} z & \alpha \\ 1 & z \end{pmatrix}^n = \begin{pmatrix} N_n(\alpha,z) & \alpha D_n(\alpha,z) \\ D_n(\alpha,z) & N_n(\alpha,z) \end{pmatrix}, \tag{2}$$

from which follows

$$\begin{pmatrix} z & \alpha \\ 1 & z \end{pmatrix}\begin{pmatrix} N_{n-1}(\alpha,z) \\ D_{n-1}(\alpha,z) \end{pmatrix} = \begin{pmatrix} N_n(\alpha,z) \\ D_n(\alpha,z) \end{pmatrix}, \quad \begin{pmatrix} N_{n-1}(\alpha,z) \\ D_{n-1}(\alpha,z) \end{pmatrix} = \begin{pmatrix} \frac{z}{z^2-\alpha} & -\frac{\alpha}{z^2-\alpha} \\ -\frac{1}{z^2-\alpha} & \frac{z}{z^2-\alpha} \end{pmatrix}\begin{pmatrix} N_n(\alpha,z) \\ D_n(\alpha,z) \end{pmatrix} \tag{3}$$

From (2), it also follows that the Rèdei polynomials are linear recurrent sequences with characteristic polynomial $t^2-2zt+z^2-\alpha$, i.e.,

$$\begin{cases} N_n(\alpha,z)=2zN_{n-1}(\alpha,z)-(z^2-\alpha)N_{n-2}(\alpha,z), & n\geq 2 \\ N_0(\alpha,z)=1, N_1(\alpha,z)=z \end{cases}, \tag{4}$$

$$\begin{cases} D_n(\alpha,z)=2zD_{n-1}(\alpha,z)-(z^2-\alpha)D_{n-2}(\alpha,z), & n\geq 2 \\ D_0(\alpha,z)=0, D_1(\alpha,z)=1 \end{cases} \tag{5}$$

Finally, we can observe that $N_n(\alpha,z)$ and $D_n(\alpha,z)$ are polynomials of degree n and $n-1$ in z, respectively. The Rédei rational functions $\dfrac{N_n(\alpha,z)}{D_n(\alpha,z)}$ have been studied and applied in several fields. For instance, they have been exploited to create public key cryptographic systems [3], [12] and to generate pseudorandom sequences [16]. Moreover, in [2], the authors used the Rédei rational functions for generating solutions of the classical Pell equation. For further properties of the Rédei polynomials, see [8].

In the classical paper of Nathanson [11], he proved that the polynomial Pell equation

$$P^2-(x^2+d)Q^2=1,$$

has non-trivial solutions $P(x),Q(x)\in\mathbb{Z}[X]$ if and only if $d=\pm1,\pm2$ and he gave these polynomials explicitly:

$$\begin{cases} A_n=\left(\frac{2}{d}x^2+1\right)A_{n-1}+\frac{2}{d}x(x^2+d)B_{n-1}, & A_0=1 \\ B_n=\frac{2}{d}xA_{n-1}+\left(\frac{2}{d}x^2+1\right)B_{n-1}, & B_0=0 \end{cases}$$

for any $n\geq 1$, when $d=1,\pm2$ and

$$\begin{cases} A'_n=xA'_{n-1}+(x^2-1)B'_{n-1}, & A'_0=1 \\ B'_n=A'_{n-1}+xB'_{n-1}, & B'_0=0 \end{cases}$$

for any $n \geq 1$, when $d = -1$. Using the Rédei polynomials, we can solve a more general case of polynomial Pell equations, where we retrieve the results of Nathanson as a particular case. In the next theorem we see that the Rédei polynomials are polynomial solutions of

$$P^2 - (f^2(x) + d)Q^2 = 1, \tag{6}$$

where $f(x)$ is any integer polynomial and $d \in \mathbb{Z}$.

Theorem 1. *Given $d \in \mathbb{Z}$ and $f \in \mathbb{Z}[X]$, consider the Rédei polynomials $N_n(x) = N_n(f^2(x) + d, f(x))$ and $D_n(x) = D_n(f^2(x) + d, f(x))$, then*

$$\left(\frac{N_n(x)}{(-d)^{n/2}}\right)^2 - (f^2(x) + d)\left(\frac{D_n(x)}{(-d)^{n/2}}\right)^2 = 1.$$

Moreover, the solutions are integer polynomials if and only if $d = 1, \pm 2$ and n even, $d = -1$ for any n.

Proof. From (2) we have

$$N_n^2(\alpha, z) - \alpha D_n^2(\alpha, z) = (z^2 - \alpha)^n,$$

for any $n \geq 1$. Considering $z = f(x)$ and $\alpha = f^2(x) + d$ we obtain

$$N_n^2(x) - (f^2(x) + d)D_n^2(x) = (-d)^n$$

i.e.,

$$\left(\frac{N_n(x)}{(-d)^{n/2}}\right)^2 - (f^2(x) + d)\left(\frac{D_n(x)}{(-d)^{n/2}}\right)^2 = 1.$$

Clearly, when $d = -1$, we have obtained solutions of the polynomial Pell equation which are integer polynomials. When $d = 1$, $\dfrac{N_n(x)}{(-d)^{n/2}}$ and $\dfrac{D_n(x)}{(-d)^{n/2}}$ are integer polynomials if and only if n is even. We complete the proof showing that $d^{[n/2]} \mid N_n(x)$ if and only if $d = \pm 2$, for any $n \geq 1$. For $n = 1$ and $n = 2$, we have

$$N_1(x) = f(x), \quad N_2(x) = 2f^2(x) + d$$

and the statement is true. Let us observe that if $d \neq \pm 2$, then $d \not| N_2(x)$. Now, we proceed by induction. From (4), we have

$$N_n(x) = 2f(x)N_{n-1}(x) + dN_{n-2}(x) = 2f(x)d^{[(n-1)/2]} \cdot a + d \cdot d^{(n-2)/2} \cdot b$$

for certain integers a and b. From the last equality, which holds by inductive hypothesis, we have that $d^{[n/2]} \mid N_n(x)$. Similarly, we can get the same result for $D_n(x)$. □

For proving that all the integer polynomial solutions of (6) are given in the previous theorem, we need the following lemma.

Lemma 1. *Let $f(x)$, $P(x)$ and $Q(x)$ be polynomials of degree m, nm and $(n-1)m$, respectively, with coefficients of the highest degree that are positive and*

$$P^2 - (f^2(x) + d)Q^2 = (-d)^n, \tag{7}$$

with $d \in \mathbb{Z}^*$. Given $P'(x) = -\dfrac{f(x)}{d}P(x) + \dfrac{f^2(x) + d}{d}Q(x)$ and $Q'(x) = \dfrac{1}{d}P(x) - \dfrac{f(x)}{d}Q(x)$ then

1. *$P'^2 - (f^2(x) + d)Q'^2 = (-d)^{n-1}$*
2. *$\deg P' < \deg P$ and $\deg Q' < \deg Q$*

Proof. 1. We have

$$P'^2 - (f^2(x)+d)Q'^2 = \frac{f^2(x)}{d^2}P^2 + \frac{(f^2(x)+d)^2}{d^2}Q^2 - (f^2(x)+d)\frac{1}{d^2}P^2 - (f^2(x)+d)\frac{f^2(x)}{d^2}Q^2 =$$

$$= -(f^2(x) + d)\frac{1}{d^2}(P^2 - (f^2(x) + d)Q^2) + \frac{f^2(x)}{d^2}(P^2 - (f^2(x) + d)Q^2) =$$

$$= -(f^2(x) + d)(-d)^{n-2} + f^2(x)(-d)^{n-2} = (-d)^{n-1}.$$

2. Since $\deg P^2 = 2nm$, $\deg f^2Q^2 = 2nm$, $\deg Q^2 = 2nm - 2m$ and it holds

$$P^2 - f^2(x)Q^2 - dQ^2 = (-d)^n$$

we have that $P^2 - f^2Q^2$ has degree $2nm - 2m$. Moreover, we can observe that the degree of $P + fQ$ is nm by the hypothesis that coefficients of the highest degree of P, f, Q are positive. Thus, from $P^2 - f^2Q^2 = (P - fQ)(P + fQ)$, we have that the coefficients of degree $nm, nm - 1, \dots nm - m$ of the polynomial $P - fQ$ are zero, i.e., $\deg Q' < \deg Q$. Similar considerations prove that $\deg P' < \deg P$.

□

Theorem 2. *All the integer polynomial solutions of*

$$P^2 - (f^2(x) + d)Q^2 = 1 \tag{8}$$

are the polynomials $N_n(x)$ and $D_n(x)$ for $d = -1$ and any n, $\frac{N_n(x)}{(-d)^{n/2}}$ and $\frac{D_n(x)}{(-d)^{n/2}}$ for $d = 1, \pm 2$ and n even.

Proof. Let $P(x)$ and $Q(x)$ be solutions of (8), if $\deg f = m$, then must be $\deg P = mn$ and $\deg Q = m(n-1)$. Now we consider the polynomials $\tilde{P}(x) = d^{n/2} \cdot P(x)$ and $\tilde{Q}(x) = d^{n/2} \cdot Q(x)$ and we show that these polynomials coincide with the Rédei one's (unless the sign). We proceed by induction on n. The basis of the induction is straightforward to check. By Lemma 1 and the inductive hypothesis $-\frac{f(x)}{d}\tilde{P}(x) + \frac{f^2(x)+d}{d}\tilde{Q}(x) = N_{n-1}(x)$ and $\frac{1}{d}\tilde{P}(x) - \frac{f(x)}{d}\tilde{Q}(x) = D_{n-1}(x)$. Let us observe that we have assumed the positivity of the highest coefficients because of the form of the equation (8), in which only the squares f^2, P^2, Q^2 appear, hence hypotheses of Lemma 1 are satisfied. Thus, from (3), we have the thesis. □

We have seen that the Rédei polynomials allow to study and solve a vast class of polynomial Pell equations in a very simple and direct way. This also generalizes the result of Nathanson [11] that we can retrieve when $f(x) = x$. Moreover, we can use the above approach for studying the most general case of polynomial Pell equations, i.e.,

$$P^2 - f(x)Q^2 = 1,$$

where f is any integer polynomial. In this case, if we consider $\alpha = f(x)$ and $z = \pm\sqrt{f(x)+1}$, surely we obtain that

$$N_n^2(x) - f(x)D_n^2(x) = 1$$

for any $n \geq 0$, where $N_n(x) = N_n(f(x), \pm\sqrt{f(x)+1})$ and $D_n(x) = D_n(f(x), \pm\sqrt{f(x)+1})$. If $f(x)$ is a polynomial such that $f(x)+1$ is a square, then the Rédei polynomials $N_n(x)$ and $D_n(x)$ are integer polynomials for any $n \geq 0$.

Question 1. *Are all the solutions of the polynomial Pell equation (1), for any $D(x) \in \mathbb{Z}[X]$, the Rédei polynomials?*

Example 1. *In the following Table 1, we write the Rédei polynomials $N_n(x^4-1, x^2)$ and $D_n(x^4-1, x^2)$, by Theorem 1 we have that they are the solutions of the polynomial Pell equation $P^2 - (x^4-1)Q^2 = 1$.*

n	$N_n(x^4-1, x^2)$	$D_n(x^4-1, x^2)$
1	x^2	1
2	$2x^4 - 1$	$2x^2$
3	$4x^6 - 3x^2$	$4x^4 - 1$
4	$8x^8 - 8x^4 + 1$	$8x^6 - 4x^2$
5	$16x^{10} - 20x^6 + 5x^2$	$16x^8 - 12x^4 + 1$

Table 1: Polynomial solutions of $P^2 - (x^4-1)Q^2 = 1$

Example 2. *In Table 2, we summarize the Rèdei polynomials $N_n(x^4+2,x^2)$ and $D_n(x^4+2,x^2)$. For obtaining integer polynomials that are the solutions of the polynomial Pell equation $P^2-(x^4+2)Q^2=1$, we have to consider the Rédei polynomials with even index n and divide them by $-2^{n/2}$. In this way we the following solutions*

$$(-x^4-1,-x^2),\quad (2x^8+4x^4+1,2x^6+2x^2),\quad (-4x^{12}-12x^8-9x^4-1,-4x^{10}-8x^6-3x^2),\dots$$

n	$N_n(x^4+2,x^2)$	$D_n(x^4+2,x^2)$
1	x^2	1
2	$2x^4+2$	$2x^2$
3	$4x^6+6x^2$	$4x^4+2$
4	$8x^8+16x^4+4$	$8x^6+8x^2$
5	$16x^{10}+40x^6+20x^2$	$16x^8+24x^4+4$
6	$32x^{12}+96x^8+72x^4+8$	$32x^{10}+64x^6+24x^2$

Table 2: Rèdei polynomials $N_n(x^4+2,x^2)$ and $D_n(x^4+2,x^2)$

Example 3. *If we consider the Rédei polynomials $N_n(x^2+3,x)$ and $D_n(x^2+3,x)$, summarized in Table 3, we have that $N_n(x^2+3,x)/(-d)^{n/2}$ and $D_n(x^2+3,x)/(-d)^{n/2}$ are the solutions of the polynomial Pell equation $P^2-(x^2+3)Q^2=1$, however, in this case, we do not have integer polynomials as solutions.*

n	$N_n(x^2+3,x)$	$D_n(x^2+3,x)$
1	x	1
2	$2x^2+3$	$2x$
3	$4x^3+9x$	$4x^2+3$
4	$8x^4+24x^2+9$	$8x^3+12x$
5	$16x^5+60x^3+45x$	$16x^4+36x^2+9$

Table 3: Rèdei polynomials $N_n(x^2+3,x)$ and $D_n(x^2+3,x)$

In the next scetion, we see that the Rédei polynomials can be generalized in a natural way and they are useful for studying polynomial Pell equations of higher degrees.

3 Polynomial Pell equation of higher degrees

The classical Pell equation can be generalized in a natural way to higher degrees. Indeed, we can observe that the Pell equation arises considering the unitary elements of the quotient filed $\mathbb{Q}[x]/(x^2-d)$, where x^2-d is an irreducible polynomial over $\mathbb{Q}$. Thus, considering the unitary elements of $\mathbb{Q}[x]/(x^3-c)$, where c is not a cube, we get the cubic Pell equation

$$x^3+cy^3+cz^3-3cxyz=1,$$

in the unknowns x,y,z. Similarly, we can construct the Pell equations of degree m that is defined by

$$\det\begin{pmatrix} x_1 & rx_m & rx_{m-1} & \dots & rx_2 \\ x_2 & x_1 & rx_m & \dots & rx_3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ x_{m-1} & x_{m-2} & \dots & x_1 & rx_m \\ x_m & x_{m-1} & x_{m-2} & \dots & x_1 \end{pmatrix}=1 \tag{9}$$

in the unknowns $x_1,\dots x_m$, where r is not a m-th power. For further details, see [1]. Thus, it is natural generalizing the study of the polynomial Pell equation to higher degrees, considering the

matrix

$$P = \begin{pmatrix} P_1 & RP_m & RP_{m-1} & \dots & RP_2 \\ P_2 & P_1 & RP_m & \dots & RP_3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ P_{m-1} & P_{m-2} & \dots & P_1 & RP_m \\ P_m & P_{m-1} & P_{m-2} & \dots & P_1 \end{pmatrix}, \quad \det P = 1, \tag{10}$$

where $P_1(x), \dots, P_m(x)$ are unknown polynomials and $R(x)$ is a given integer polynomial. Gaunet [5] studied the polynomial cubic Pell equation

$$P_1^3 + RP_2^3 + R^2P_3^3 - 3RP_1P_2P_3 = 1 \tag{11}$$

when $R(x) = x^3 + ax + b$, characterizing when the equation admits non-trivial solutions and finding them. Here, we study the general polynomial Pell equation of degree m, given by equation (10), where $P_1, \dots P_m$ are unknown polynomial in $\mathbb{Z}[X]$ and $R(x) = f(x) + r$, with $f(x)$ is any integer polynomial and $r \in \mathbb{Z}$. As a particular case we obtain solutions of the equation (11) for a different class of polynomials R.

We define the *generalized Rédei polynomials* by means of

$$(z + \sqrt[m]{\alpha})^n = A_n^{(0)}(z,\alpha) + A_n^{(1)}(z,\alpha)\sqrt[m]{\alpha} + \dots + A_n^{(m-1)}(z,\alpha)\sqrt[m]{\alpha^{m-1}}.$$

In the following, when there is no confusion, we omit the dependence on z, α when we write the generalized Rédei polynomials for the seek of simplicity. The generalized Rédei polynomials can be obtained by the powers of a particular $m \times m$ matrix. Indeed, by definition, we have

$$A_{n+1}^{(0)} + A_{n+1}^{(1)}\sqrt[m]{\alpha} + \dots + A_{n+1}^{(m-1)}\sqrt[m]{\alpha^{m-1}} = (A_n^{(0)} + A_n^{(1)}\sqrt[m]{\alpha} + \dots + A_n^{(m-1)}\sqrt[m]{\alpha^{m-1}})(z + \sqrt[m]{\alpha})$$

i.e.

$$A_{n+1}^{(0)} = zA_n^{(0)} + \alpha A_n^{(m-1)}, \quad A_{n+1}^{(i)} = zA_n^i + A_n^{(i-1)}, \quad i = 1, \dots, m-1.$$

Thus, given the matrix

$$M = \begin{pmatrix} z & 0 & 0 & \dots & \alpha \\ 1 & z & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & z & 0 \\ 0 & \dots & 0 & 1 & z \end{pmatrix} \tag{12}$$

we can write

$$M \begin{pmatrix} A_n^{(0)} \\ \vdots \\ A_n^{(m-1)} \end{pmatrix} = \begin{pmatrix} A_{n+1}^{(0)} \\ \vdots \\ A_{n+1}^{(m-1)} \end{pmatrix}$$

from which

$$M^n = \begin{pmatrix} A_n^{(0)} & \alpha A_n^{(m-1)} & \dots & \alpha A_n^{(1)} \\ A_n^{(1)} & A_n^{(0)} & \dots & \alpha A_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_n^{(m-1)} & A_n^{(m-2)} & \dots & A_n^{(0)} \end{pmatrix}. \tag{13}$$

From (12), we can observe that $\det M^n = (z^m + (-1)^{m-1}\alpha)^n$, on the other hand, from (13) we have that $\det M^n = \det P$ when $P_1 = A_n^{(0)}, \dots, P_m = A_n^{(m-1)}$ and $R = \alpha$. Thus, the generalized Rédei polynomials can be exploited for solving the polynomial Pell equation of higher degrees for convenient choices of z and α. Indeed, if $z = f(x) \in \mathbb{Z}[x]$ and $\alpha = (-f(x))^m + r$, with $r \in \mathbb{Z}$, then the Rédei polynomials satisfy the polynomial equation $\det P = ((-1)^{m-1}r)^n$, where $R(x) = (-f(x))^m + r$, and the polynomials $\dfrac{A_n^{(0)}(x)}{((-1)^{m-1}r)^{n/m}}, \dots, \dfrac{A_n^{(m-1)}(x)}{((-1)^{m-1}r)^{n/m}}$ satisfy the polynomial Pell equation $\det X = 1$, for $R(x) = (-f(x))^m + r$. However, these solutions are not ever integer polynomials. They are integer polynomials in the following cases

1. $r = -1$ and any $n \geq 0$,

2. $r = 1$ and any $n \equiv 0 \pmod{m}$,

3. $r = \pm m$ and any $n \equiv 0 \pmod{m}$, when m is a prime number.

The situations 1 and 2 are immediate to verify. Let us focus on situation 3. We can observe that

$$A_1^{(0)}(x) = f(x), A_2^{(0)}(x) = f^2(x), \ldots, A_{m-1}^{(0)}(x) = f^{m-1}(x), A_m^{(0)}(x) = \pm m$$

Moreover, the characteristic polynomial of M is

$$x^m + \sum_{i=1}^{m-1} (-1)^i \binom{m}{i} x^{m-i} f^i(x) \pm m,$$

thus if m is prime, we have

$$\pm m | A_m^{(0)}(x), \pm m | A_{m+1}^{(0)}(x), \ldots, \pm m | A_{2m-1}^{(0)}(x)$$

and consequently $m^2 | A_{2m}^{(0)}(x)$. Thus we can prove by induction that the Rédei polynomials are in $\mathbb{Z}[x]$ for $r = \pm m$ and any $n \equiv 0 \pmod{m}$, when m is a prime number.

Question 2. *Are all the integer polynomial solutions of* (10)*, for* $R(x) = (-f(x))^m + r$*, the Rédei polynomials?*

Acknowledgments

The author is really grateful to the anonymous referee for the carefully reading of the paper and for all the suggestions that improved the presentation of the paper.

References

[1] E. J. Barbeau, Pell's equation, Springer, New York, 2003.

[2] S. Barbero, U. Cerruti, N. Murru, Solving the Pell equation via Rédei rational functions, The Fibonacci Quarterly, Vol. 48, 348–357, 2010.

[3] E. Bellini, N. Murru, An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics, Finite Fields and their Applications, Vol. 39, 179–194, 2016.

[4] A. Dubickas, J. Steuding, The polynomial Pell equation, Elem. Math., Vol. 59, 133–143, 2004.

[5] M. L. Gaunet, Formes cubiques polynomiales, C. R. Acad. Sci. Paris, Vol. 311, 491–494, 1990.

[6] J. C. Griffin, G. Gunatillake, Orthogonal-type poltnomials and Pell equations, Integral Transforms and Special Functions, Vol. 24, 796–806, 2013.

[7] F. Hazama, Pell equations for polynomials, Indag. Mathem., Vol. 8, 387–397, 1997.

[8] R. Lidl, G. L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monogr. Surveys Pure appl. Math. 65, Longman, 1993.

[9] J. Mc Laughlin, Polynomial solutions to Pell's equation and fundamental units in real quadratic fields, Journal of the London Mathematical Society, Vol. 67, 16-28, 2003.

[10] R. A. Mollin, Polynomial solutions for Pell's equation revisited, Indian J. Pure Appl. Math., Vol. 28, 429–438, 1997.

[11] M. B. Nathanson, Polynomial Pell's equation, Proceedings of the American Mathematical Society, Vol. 86, 89–92, 1976.

[12] R. Nobauer, Cryptanalysis of the Rédei scheme, Contributions to General Algebra, Vol. 3, 255–264, 1984.

[13] A. V. Pastor, Generalized Chebyshev polynomials and the Pell–Abel equation, Fundam. Prikl. Mat., Vol. 7, 1123–1145, 2001.

[14] A. M. S. Ramasamy, Polynomial solutions for the Pell's equation, Indian J. Pure Appl. Math., Vol. 25, 577–581, 1994.

[15] L. Rédei, Über eindeuting umkehrbare polynome in endlichen korpen, Acta Sci. Math. (Szeged), Vol. 11, 85–92, 1946.

[16] A. Topuzoglu, A. Winterhof, Topics in geometry, coding theory and cryptography, Algebra and Applications, Vol. 6, 135–166, 2006.

[17] W. A. Webb, H. Yokota, Polynomial Pell's equation, Proceedning of the American Mathematical Society, Vol. 131, 993–1006, 2003.

[18] W. A. Webb, H. Yokota, Polynomial Pell's equation II, Journal of Number Theory, Vol. 106, 128–141, 2004.

[19] H. Yokota, Solutions of polynomial Pell's equation, Journal of Number Theory, Vol. 130, 2003–2010, 2010.

[20] L. Zapponi, Parametric solutions of Pell equations, Proc. of the Roman Number Theory Association, Vol. 1, 43–48, 2016.