The Quadratic Diophantine Equations $x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0$

Amara Chandoul[1,2], Diego Marques[1], Samira Shaban Albrbar[3]

[1] Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro Brasília - DF 70910-900, Brazil

[2] Higher Institute of Informatics and Multimedia of Sfax, Sfax University, Tunisia

[3] Curtin University of Technology, Department of Mathematics and statistics, Bentley Campus, Kent Street Bentley, WA 6102, Western Australia

Correspondence: Amara Chandoul, Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro Brasília - DF 70910-900, Brazil. E-mail: amarachandoul@yahoo.fr

Received: January 11, 2019 Accepted: February 13, 2019 Online Published: February 20, 2019

doi:10.5539/jmr.v11n2p30 URL: https://doi.org/10.5539/jmr.v11n2p30

Abstract

Let $P := P(t)$ be a non square polynomial. In this paper, we consider the number of integer solutions of Diophantine equation

$$E \ : \ x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0.$$

We derive some recurrence relations on the integer solutions (x_n, y_n) of E. In the last section, we consider the same problem over finite fields F_p for primes $p \geq 5$. Our main results are generaliations of previous results given by Ozcok and Tekcan (Ozkoc and Tekcan, 2010).

Keywords: Diophantine equation, Pell's equation, continued fraction, quadratic residue

1. Introduction

Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients in one or more variables. A Diophantine equation is an algebraic equation

$$f(x_1, x_2, \ldots, x_n) = 0$$

for which integer solutions are sought.

The problem to be solved is to determine whether or not a given Diophantine equation has solutions in the domain of integer numbers.

In the case where the Diophantine equation is solvable, there are some natural questions:

$*$) Is the number of solutions finite or infinite ?

$**$) Is it possible to determine all solutions ?

In 1900, (Hilbert, 1900), asked for general algorithm to determine, in a finite number of steps, the solvability of any given Diophantine equation. In other words, he asked if there are any universal method of solving all Diophantine equations.

Unfortunately, it was proven by Matyasevich, in 1970, that this problem is unsolvable (Matyasevich, 1970).

The absence of a general algorithm was not by itself obstacle to involve more than technique in solving Diophantine equations. In fact, Diophantine equations can be very creative and mathematiciens usually have to exhibit creativity to solve these questions.

One of the best-known techniques is that one based on reduction of the Diophantine equation of arbitrary size with many arbitrary unknowns to another equation having a fixed degree and fixed number of unknowns.

Another one of the most common techniques used to examine Diophantine equations problem is that based on considering residues by checking certain common modulos on each term of the equation, one can either arrive at a contradiction to prove that there's no solution, or to find the unique solutions that satisfy the equation. This technique assumes basic knowledge of modular arithmetic as well as important notions and theorem like the quadratic residues modulo a prime number p and Euler theorem.

Recently, there are a number of paper have been written and published by Tekcan and Chandoul, using the techniques mentioned above, see (Tekcan, 2004, 2006, 2007, 2010, 2011 and Chandoul, 2011).

This paper offers an extension of one of the results given by Ozkoc and Tekcan, that is given in (Ozkoc and Tekcan, 2010). In (Ozkoc and Tekcan, 2010), Tekcan consider the number of integer solutions of Diophantine equation E : $x^2 - (t^2 - t)y^2 - (4t - 2)x + (4t^2 - 4t)y = 0$ over $\mathbb{Z}$, where $t \geq 2$. Then, we assume that the Diophantine equation E can be extended to the form

$$E : \ x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0$$

where $P(t)$ be a non-square polynomial.

These extensions allows us to solve many types of such equations. We also derive some recurrence relations on the integer solutions of a Pell equation.

Another advantage of our results is that the procedure can be implemented by computer, which allows us to obtain all the solutions after the insertion of the coefficients and the verification of the conditions of the method.

2. Main Results

We consider the equation

$$E : \ x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0 \tag{2.1}$$

with $P := P(t) \in \mathbb{Z}[t]\backslash\{0, 1\}$ a non square polynomial. It is a generalization of the quadratic Diophantine equation given by Ozkoc and Tekcan, (Ozkoc and Tekcan, 2010). Here, we show that: if P is a non perfect square polynomial, then (2.1) has an infinitude of integer solutions. In this case we find a closed expression (x_n, y_n), the general positive integer solution, by an original method.

Note that the resolution of E in its present form is difficult, that is, we can not determine how many solutions E has and what they are. So, we have to transform E into a Pell equation which can be easily solved. To get this let

$$T \ : \ \begin{cases} x = u + P'(t) \\ y = v + 2 \end{cases} \tag{2.2}$$

we get,

$$\begin{aligned} T(E) \ := \widetilde{E} : \quad & (u + P'(t))^2 - P(t)(v + 2)^2 - 2P'(t)(u + P'(t)) + 4P(t)(v + 2) \\ & +(P'(t))^2 - 4P(t) - 1 = 0 \end{aligned}$$

Then, the equation (2.1) becomes

$$\widetilde{E} \ : \ u^2 - P(t)v^2 = 1 \tag{2.3}$$

which is a Pell equation.

It is known that the above Pell equation is always solvable. Its solutions are related to the continued fraction expansion of $\sqrt{P(t)}$.

We will be concerned with the continued fraction expansions of $\sqrt{P(t)}$, where $P(t)$ is a non-square. In fact, this continued fractions have a very interesting form, which is summarized in the next theorem.

Theorem 2.1 Let $P(t)$ be a prime. Then $\sqrt{P(t)} = [a_0; a_1, a_2, \cdots, a_l, 2a_0]$, where the repeating portion, excluding the last term, is symmetric upon reversal, and the central term may appear either once or twice.

Theorem 2.2 Let $\sqrt{P(t)} = \left[a_0; \overline{a_1, a_2, \cdots, a_l, 2a_0}\right]$ denote the continued fraction expansion of period lenght l, where $P(t)$ be a non-square polynomial.

Let $\dfrac{p_n}{q_n}$ be the nth convergent of $\sqrt{P(t)}$. Then

(1) The fundamental solution of the Pell equation $\widetilde{E}$ in (2.3) is (u_1, v_1), such that

$$\begin{cases} u_1 = p_{l-1} \\ \\ v_1 = q_{l-1} \end{cases}, \text{ if } l \text{ is even}, \quad \text{and} \quad \begin{cases} u_1 = p_{2l-1} \\ \\ v_1 = q_{2l-1} \end{cases}, \text{ if } l \text{ is even}$$

Set $\{(u_k, v_k)\} = \{(p_{kl-1}, q_{kl-1})\}$ where

$$\frac{p_{kl-1}}{q_{kl-1}} = \left[a_0;\ \underbrace{a_1, a_2, \cdots, a_l}_{l-1},\ 2a_0,\ \underbrace{a_1, a_2, \cdots, a_l, 2a_0, a_1, a_2, \cdots, a_l}_{(k-1)l-1}\right], \text{ if } l \text{ is even.}$$

$$\text{And } \frac{p_{2kl-1}}{q_{2kl-1}} = \left[a_0; \underbrace{a_1, \cdots, a_l, 2a_0, a_1, \cdots, a_l}_{2l-1}, 2a_0, \underbrace{a_1, \cdots, a_l, 2a_0, \cdots, a_1, \cdots, a_l}_{(2k-2)l-1},\right], \text{ if } l \text{ is odd.}$$

Then (u_k, v_k) is a solution of $\widetilde{E}$.

(2) The consecutive solutions (u_{k-1}, v_{k-1}) and (u_k, v_k) the Pell equation $\widetilde{E}$ in (2.3) satisfy

$$\begin{cases} u_k = u_1 u_{k-1} + (a_0 u_1 + \alpha) v_{k-1} \\ \\ v_k = v_1 u_{k-1} + (a_0 v_1 + \beta) v_{k-1} \end{cases}, \text{ forall } k \geq 2, \quad \text{if } l \text{ is even}$$

where $\alpha = x_{l-2}$ and $\beta = x_{l-2}$.

and

$$\begin{cases} u_k = u_1 u_{k-1} + (a_0 u_1 + \eta) v_{k-1} \\ \\ v_k = v_1 u_{k-1} + (a_0 v_1 + \delta) v_{k-1} \end{cases}, \text{ forall } k \geq 2, \quad \text{if } l \text{ is odd}$$

where $\eta = x_{2l-2}$ and $\delta = x_{2l-2}$.

To prove this theorem, we need the following Lemma

Lemma 2.3 Let $\sqrt{P(t)} = \left[a_0; \overline{a_1, a_2, \cdots, a_l, 2a_0}\right]$ denote the continued fraction expansion of period lenght l. Then

$$\begin{cases} a_0 x_{kl-1} + x_{kl-2} = P(t) y_{kl-1} \\ a_0 y_{kl-1} + y_{kl-2} = x_{kl-1} \end{cases}$$

for all $k \geq 2$.

Proof. (Lemma 2.3)

We have $\sqrt{P(t)} = \left[a_0; \overline{a_1, a_2, \cdots, a_1, 2a_0}\right]$. Thus, we may write $\sqrt{P(t)} = \left[a_0; a_1, a_2, \cdots, a_{kl-1}, a_0 + \sqrt{P(t)}\right]$, then $\sqrt{P(t)} = \dfrac{(a_0 + \sqrt{P(t)}) x_{kl-1} + x_{kl-2}}{(a_0 + \sqrt{P(t)}) y_{kl-1} + y_{kl-2}}$, which gives rise to the equation

$$P(t) y_{kl-1} + \sqrt{P(t)}(a_0 y_{kl-1} + y_{kl-2}) = (a_0 x_{kl-1} + x_{kl-2}) + \sqrt{P(t)} x_{kl-1}.$$

Which yields, $a_0 x_{kl-1} + x_{kl-2} = P(t) y_{kl-1}$ and $a_0 y_{kl-1} + y_{kl-2} = x_{kl-1}$.

□

Proof. (Theorem 2.2)

(1) We prove the theorem only for even number l. It is easily seen that $x_{kl-1}^2 - P(t) y_{kl-1}^2 = x_{kl-1} y_{kl-1} - y_{kl-1} x_{kl-2}$, which gives $x_{kl-1}^2 - P(t) y_{kl-1}^2 = (-1)^{kl}$. Thus, if l is even $x_{kl-1}^2 - P(t) y_{kl-1}^2 = 1$ which yields (u_k, v_k) are solutions of $\widetilde{E}$ for all $k \geq 1$ and (u_1, v_1) is the fundamental solution.

We can also prove it using the method of mathematical induction. In fact, if l is even, we have

$$\begin{aligned}
\frac{u_k}{v_k} = \frac{x_{kl-1}}{y_{kl-1}} &= \left[a_0; \underbrace{a_1, a_2, \cdots, a_1}_{l-1}, 2a_0, \underbrace{a_1, a_2, \cdots, a_1, 2a_0, \cdots, a_1, a_2, \cdots, a_1}_{(k-1)l-1}\right] \\
&= \left[a_0; \underbrace{a_1, a_2, \cdots, a_1}_{l-1}, a_0 + a_0, \underbrace{a_1, a_2, \cdots, a_1, 2a_0, \cdots, a_1, \cdots, a_1}_{(k-1)l-1}\right] \\
&= \left[a_0; \underbrace{a_1, a_2, \cdots, a_1}_{l-1}, a_0 + \frac{x_{(k-1)l-1}}{y_{(k-1)l-1}}\right] \quad . \\
&= \frac{\left(a_0 + \dfrac{x_{(k-1)l-1}}{y_{(k-1)l-1}}\right) x_{l-1} + x_{l-2}}{\left(a_0 + \dfrac{x_{(k-1)l-1}}{y_{(k-1)l-1}}\right) y_{l-1} + y_{l-2}} \\
&= \frac{a_0 y_{(k-1)l-1} x_{l-1} + x_{(k-1)l-1} x_{l-1} + y_{(k-1)l-1} x_{l-2}}{a_0 y_{(k-1)l-1} y_{l-1} + x_{(k-1)l-1} y_{l-1} + y_{(k-1)l-1} y_{l-2}}
\end{aligned}$$

Then

$$\begin{aligned}
u_k^2 - P(t)v_k^2 &= (a_0 y_{(k-1)l-1} x_{l-1} + x_{(k-1)l-1} x_{l-1} + y_{(k-1)l-1} x_{l-2})^2 \\
&\quad -P(t)(a_0 y_{(k-1)l-1} y_{l-1} + x_{(k-1)l-1} y_{l-1} + y_{(k-1)l-1} y_{l-2})^2 \\
&= (u_1 u_{k-1} + (a_0 u_1 + \alpha) v_{k-1})^2 - P(t)(v_1 u_{k-1} + (a_0 v_1 + \beta) v_{k-1})^2 \\
&= u_1^2 u_{k-1}^2 + 2u_1(a_0 u_1 + \alpha) u_{k-1} v_{k-1} + (a_0 u_1 + \alpha)^2 v_{k-1}^2 \\
&\quad -P(t) v_1^2 u_{k-1}^2 - 2P(t)(a_0 v_1 + \beta) v_1 u_{k-1} v_{k-1} - P(t)(a_0 v_1 + \beta)^2 v_{k-1}^2 \\
&= (u_1^2 - P(t) v_1^2) u_{k-1}^2 - \left[(P(t)(a_0 v_1 + \beta)^2 - (a_0 u_1 + \alpha)^2\right] v_{k-1}^2 \\
&\quad +2\left[u_1(a_0 u_1 + \alpha) - P(t) v_1 (a_0 v_1 + \beta)\right] u_{k-1} v_{k-1}
\end{aligned}$$

Using the above lemma (Lemma 2.3), we have

$(P(t)(a_0 v_1 + \beta)^2 - (a_0 u_1 + \alpha)^2 = P(t) u_1^2 - P(t)^2 v_1^2 = P(t)(u_1^2 - P(t) v_1^2) = P(t)$ and $u_1(a_0 u_1 + \alpha) - P(t) v_1 (a_0 v_1 + \beta) = 0$. Hence, we conclude that

$$u_k^2 - P(t) v_k^2 = u_{k-1}^2 - P(t) v_{k-1}^2 = 1$$

So (u_k, v_k) is also solution of $\widetilde{E}$. Completing the proof.
(2) This assertion is clear by the above. □

As we reported above, the Diophantine equation E could be transformed into the Diophantine equation $\tilde{E}$ via the transformation T. Also, we showed that $x = u + P'(t)$ and $y = v + 2$. So, we can retransfer all results from $\tilde{E}$ to E by applying the inverse of T. Thus, we can give the following main theorem

Theorem 2.4 Let D be the Diophantine equation in (2.1). Then

(1) The fundamental (minimal) solution of E is $(x_1, y_1) = (u_1 + P'(t), v_1 + 2)$

(2) Define the sequence $\{(x_n, y_n)\}_{n \geq 1} = \{(u_n + P'(t), v_n + 2)\}$, where $\{(x_n, y_n)\}$ defined in (**??**). Then (x_n, y_n) is a solution of E. So it has infinitely many integer solutions $(x_n, y_n) \in \mathbb{Z} \times \mathbb{Z}$.

(3) The solutions (x_n, y_n) satisfy the recurrence relations

$$\begin{cases} x_k = u_1 x_{k-1} + (a_0 u_1 + \alpha) y_{n-1} - u_1(2a_0 + P'(t)) - 2\alpha + P'(t) \\ y_k = v_1 x_{k-1} + (a_0 v_1 + \beta) y_{n-1} - v_1(2a_0 + P'(t)) - 2\beta + 2 \end{cases}, \text{ if } l \text{ is even}$$

for $k \geq 2$,and

$$\begin{cases} x_k = u_1 x_{k-1} + (a_0 u_1 + \eta) y_{n-1} - u_1(2a_0 + P'(t)) - 2\eta + P'(t) \\ y_k = v_1 x_{k-1} + (a_0 v_1 + \delta) y_{n-1} - v_1(2a_0 + P'(t)) - 2\delta + 2 \end{cases}, \text{ if } l \text{ is odd}$$

for $k \geq 2$.

Example 2.5 Let $P(t) = t^4 + 4t^3 + 6t^2 + 4t + 2$, Then

$$\sqrt{P(t)} = \left[t^2 + 2t + 1; \overline{2t^2 + 4t + 2}\right].$$

So, $(u_1, v_1) = (2t^4 + 8t^3 + 4t^2 + 3, 2t^2 + 4t + 2)$ is the fundamental solution of

$$\widetilde{E_1} \ : \ u^2 - (t^4 + 4t^3 + 2t^2 + 2)v^2 = 1$$

and the other solutions are given by

$$\begin{cases} u_k = (2t^4 + 8t^3 + 4t^2 + 3)u_{k-1} + (2t^6 + 12t^5 + 30t^4 + 40t^3 + 32t^2 + 16t + 4)v_{k-1} \\ v_k = (2t^2 + 4t + 2)u_{k-1} + (2t^4 + 8t^3 + 4t^2 + 3)v_{k-1} \end{cases}$$

For $k \geq 2$.

Morover, let $n = t^2 + 2t + 1$, then $P(t)$ become $D(n) = n^2 + 1$. Then

$$\sqrt{D(n)} = \left[n; \overline{2n}\right].$$

So, $(u_1, v_1) = (2n^2 + 1, 2n)$ is the fundamental solution of

$$\widetilde{E_1} \ : \ u^2 - (n^2 + 1)v^2 = 1$$

and the other solutions are given by

$$\begin{cases} u_k = (2n^2 + 1)u_{k-1} + (2n^3 + 2n)v_{k-1} \\ v_k = 2nu_{k-1} + (2n^2 + 1)v_{k-1} \end{cases}$$

For $k \geq 2$.

Then the fundamental solution of

$$E_1 \ : x^2 - (n^2 + 1)y^2 - 4nx + (4n^2 + 4)y - 2 = 0$$

is $(x_1, y_1) = (2n^2 + 2n + 1, 2n + 2)$ and the other solutions are given, for $k \geq 2$, by

$$\begin{cases} x_k = (2n^2 + 1)x_{k-1} + (2n^3 + 2n)y_{k-1} - 8n^3 - 4n \\ y_k = 2nx_{k-1} + (2n^2 + 1)y_{k-1} - 8n^2 + 2n - 2. \end{cases}$$

Further, for $t = 1$, $P(t) = 17$. Then

$$\sqrt{P(t)} = \left[4; \overline{8}\right].$$

So, $(u_1, v_1) = (33, 8)$ is the fundamental solution of

$$\widetilde{E_1} \ : \ u^2 - 17v^2 = 1$$

and the other solutions are given by

$$\begin{cases} u_k = 33u_{k-1} + 136v_{k-1} \\ v_k = 8u_{k-1} + 33v_{k-1} \end{cases}$$

For $k \geq 2$.

Then the fundamental solution of

$$E_1 \ : x^2 - 17y^2 - 64x + 68y + 955 = 0$$

is $(x_1, y_1) = (65, 10)$ and the other solutions are given, for $k \geq 2$, by

$$\begin{cases} x_k = 33x_{k-1} + 136y_{k-1} - 1296 \\ y_k = 8x_{k-1} + 33y_{k-1} - 320. \end{cases}$$

Example 2.6 In this example, we consider the number of integer solutions of the Diophantine equation

$$E \ : x^2 - (t^2 + t)y^2 - (4t + 2)x + (4t^2 + 4t)y = 0$$

We have $P(t) = t^2 + t$, thus $P'(t) = 2t + 1$ and the continued fraction expansion of $\sqrt{P(t)}$ is

$$\sqrt{P(t)} = \left[t; \overline{2, 2t}\right]$$

which yields, $\frac{u_1}{v_1} = [t; 2] = \frac{2t+1}{2}$. Then the fundamental solution of E is $(x_1, y_1) = (2t + 1 + P'(t), 2 + 2) = (4t + 2, 4)$ and the other solutions are given by

$$\begin{cases} x_k = (2t + 1)x_{k-1} + (2t^2 + 2t)y_{k-1} - 8t^2 - 6t \\ \\ y_k = 2x_{k-1} + (2t + 1)y_{k-1} - 8t - 2 \end{cases} \quad \text{for, } k \geq 2$$

3. The Diophantine Equation E Over Finite Fields $\mathbb{F}_p$

We will first consider the notion of a square modulo an odd prime. Let p be an odd prime and $a \in \mathbb{Z}$ such that $(a, p) = 1$. If $x^2 \equiv a \pmod{p}$ admits a solution, then a is a quadratic residue modulo p. Otherwise, a is a quadratic non residue modulo p.

In this section, we will consider the integer solutions of

$$E \ : \ x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0$$

over finite fields $\mathbb{F}_p$ for primes p. We set

$$E(\mathbb{F}_p) = \begin{array}{l} \{ \ (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \ : \ x^2 - P(t)y^2 - 2P'(t)x \ + \ 4P(t)y + (P'(t))^2 \\ -4P(t) - 1 \equiv 0 \ (\text{mod } p) \ \}. \end{array}$$

Then we can give the following theorem.

Theorem 3.1 Let E be the above Diophantine equation and $t \in \mathbb{F}_p$, then

1) If $P(t) \in Q_p$, we have

$$\#E(\mathbb{F}_p) = p - 1$$

(2) If $P(t) \notin Q_p$, we have

$$\#E(\mathbb{F}_p) = \begin{cases} p - 1, & if \ p \equiv 1 \ (\text{mod } 4) \\ \\ p + 1, & if \ p \equiv 3 \ (\text{mod } 4) \end{cases}$$

where Q_p denote the set of quadratic residues.

To prove this theorem, we need the following Lemmas:

Lemma 3.2 In every complete system of ordinary residues modulo p, there are exactly $\frac{p-2}{2}$ quadratic residues.

Proof. It suffices to prove that in $[1, p - 1]$ there are exactly $\frac{p-2}{2}$ quadratic residues. Note first that $1^2, 2^2, \ldots, (\frac{p-2}{2})^2$ are all incongruent mod p (if $1 \leq i, j < \frac{p}{2}$ and $i^2 \equiv j^2 \pmod{p}$ then $i \equiv j \pmod{p}$ hence $i = j$ or $i = -j$, i.e., $i + j \equiv 0$. But $2 \leq i + j < p$, and so $i + j \equiv 0$ is impossible).

Let S denote the set of minimal non-negative ordinary residues mod p of $1^2, 2^2, \ldots, (\frac{p-2}{2})^2$. The elements of S are quadratic residues of p and $|S| = \frac{p-2}{2}$. Suppose that $n \in [1, p - 1]$ is a quadratic residue of p. Then there exists $m \in [1, p - 1]$ such that $m^2 \equiv n$. Then $(p - m)^2 \equiv m^2 \equiv n$ and $\{m, p - m\} \cap [1, p - 1] \neq \emptyset$. Hence $n \in S$, whence S is the set of quadratic residues of p inside $[1, p - 1]$. □

Lemma 3.3 Suppose p is an odd prime; and suppose $a, \ b$ are coprime to p. Then

1) If both of $a, \ b$, or neither, are quadratic residues, then ab is a quadratic residue.

2) If one of $a, \ b$ is a quadratic residue and the other is a quadratic non-residue then ab is a quadratic non-residue.

Proof. Suppose a is a quadratic residue. As b runs over the non-zero residues mod p, so does ab. We know that ab is a quadratic residue if b is a quadratic residue, and we know that just half the non-zero residues are quadratic residues. It follows that ab must be a quadratic non-residue if b is a quadratic non-residue.

Now suppose a is a quadratic non-residue. We have just seen that if b is a quadratic residue then ab is a quadratic non-residues. But we know that only half the residues are quadratic non-residues. It follows that ab must be a quadratic residue in the remaining cases, when b is a quadratic non-residue.

□

Lemma 3.4 Let p be a prime number, then -1 is a quadratic residue modulo p, if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. Clearly -1 is a quadratic residue modulo 2. If p is odd, Apply Euler's criterion, to write $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, and notice that this is $+1$ when $(p-1)/2$ is even and -1 when $(p-1)/2$ is odd. □

Following the above lemmas, the multiplicative inverse of a residue is a residue, and the inverse of a nonresidue is a nonresidue.

Proof. (of Theorem 3.1) Now, we consider the Diophantine equation

$$E \ : \ x^2 - P(t)y^2 - 2P'(t)x + 4P(t)y + (P'(t))^2 - 4P(t) - 1 = 0,$$

over finite fields $\mathbb{F}_p$.
To prove such theorem, we reduce problem of the Diophantine equation E to problem of the Pell equation $\widetilde{E}$. In fact, it is clear that E become

$$\widetilde{E} \ : \ u^2 - P(t)v^2 = 1.$$

Now, let $t \in \mathbb{F}_p^*$ and let d such that $P(t) \equiv d \pmod p$, then $\widetilde{E}$ become

$$\widetilde{E}_{d,p} \ : \ u^2 - dv^2 \equiv 1 \pmod p$$

We set

$$\widetilde{E}_{d,p}(\mathbb{F}_p) = \left\{ \ (u,v) \in \mathbb{F}_p \times \mathbb{F}_p \ : \ u^2 - dv^2 \equiv 1 \pmod p \right\}.$$

Then, it is desired to count $\#\widetilde{E}_{d,p}(\mathbb{F}_p)$. Let $p \geq 5$, then we have two cases:

Case 1 : If $d \in Q_p$; Suppose that $v = 0$, then $\widetilde{E}_{d,p}$ become $u^2 \equiv 1 \pmod p$ and hence $u = 1$ or $u = p-1$, thus $(1,0)$ and $(p-1,0)$ are two solutions of $\widetilde{E}_{d,p}$.

Now, Suppose that $u = 0$, then $\widetilde{E}_{d,p}$ become $-dv^2 \equiv 1 \pmod p$ which yields $dv^2 \equiv -1 \pmod p$, thus $v^2 \equiv (-1)d^{-1} \pmod p$. Here we have two prospects; either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

$*$) If $p \equiv 1 \pmod 4$. Using the above lemmas, then $\widetilde{E}_{d,p}$ has two solutions $(0, v_1)$ and $(0, v_2)$. And then, we consider the set $S_p = \mathbb{F}_p \setminus \{0, 1, p-1\}$. Thus, there are $\frac{p-5}{2}$ points u in S_p such that $\frac{u^2-1}{d}$ is a square. Set $c \neq 0$ such that $\frac{u^2-1}{d} = c^2$, then $dv^2 \equiv c^2 \pmod p$, which gives that $\widetilde{E}_{d,p}$ has two solutions $(0,c)$ and $(0,-c)$ for each $u \in S_p$. So, it has $p-5$ solutions over $S_p \times S_p$. Therefore, $\widetilde{E}_{d,p}$ has $p-5+4 = p-1$ solutions over $\mathbb{F}_p$.

$**$) Suppose now that, $p \equiv 3 \pmod 4$. Using the above lemmas, then $\widetilde{E}_{d,p}$ has no solution. And then, we consider the set $S_p = \mathbb{F}_p \setminus \{0, 1, p-1\}$. Thus, there are $\frac{p-3}{2}$ points u in S_p such that $\frac{u^2-1}{d}$ is a square. Set $c \neq 0$ such that $\frac{u^2-1}{d} = c^2$, then $dv^2 \equiv c^2 \pmod p$, which gives that $\widetilde{E}_{d,p}$ has two solutions $(0,c)$ and $(0,-c)$ for each $u \in S_p$. So, it has $p-3$ solutions over $S_p \times S_p$. Therefore, $\widetilde{E}_{d,p}$ has $p-3+2 = p-1$ solutions over $\mathbb{F}_p$.

Case 2 : If $d \notin Q_p$; Suppose that $v = 0$, then $\widetilde{E}_{d,p}$ become $u^2 \equiv 1 \pmod p$ and hence $u = 1$ or $u = p-1$, thus $(1,0)$ and $(p-1,0)$ are two solutions of $\widetilde{E}_{d,p}$.

Now, Suppose that $u = 0$, then $\widetilde{E}_{d,p}$ become $-dv^2 \equiv 1 \pmod p$ which yields $dv^2 \equiv -1 \pmod p$, thus $v^2 \equiv (-1)d^{-1} \pmod p$. Here we have two prospects; either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

$*$) If $p \equiv 1 \pmod 4$. Using the above lemmas, then $\widetilde{E}_{d,p}$ has no solution. And then, we consider the set $S_p = \mathbb{F}_p \setminus \{0, 1, p-1\}$. Thus, there are $\dfrac{p-3}{2}$ points u in S_p such that $\dfrac{u^2-1}{d}$ is a square. Set $c \neq 0$ such that $\dfrac{u^2-1}{d} = c^2$, then $dv^2 \equiv c^2 \pmod p$, which gives that $\widetilde{E}_{d,p}$ has two solutions $(0, c)$ and $(0, -c)$ for each $u \in S_p$. So, it has $p-3$ solutions over $S_p \times S_p$. Therefore, $\widetilde{E}_{d,p}$ has $p-3+2 = p-1$ solutions over $\mathbb{F}_p$.

$**$) Suppose now that, $p \equiv 3 \pmod 4$. Using the above lemmas, then $\widetilde{E}_{d,p}$ has two solutions. And then, we consider the set $S_p = \mathbb{F}_p \setminus \{0, 1, p-1\}$. Thus, there are $\dfrac{p-3}{2}$ points u in S_p such that $\dfrac{u^2-1}{d}$ is a square. Set $c \neq 0$ such that $\dfrac{u^2-1}{d} = c^2$, then $dv^2 \equiv c^2 \pmod p$, which gives that $\widetilde{E}_{d,p}$ has two solutions $(0, c)$ and $(0, -c)$ for each $u \in S_p$. So, it has $p-3$ solutions over $S_p \times S_p$. Therefore, $\widetilde{E}_{d,p}$ has $p-3+4 = p+1$ solutions over $\mathbb{F}_p$. □

Note that ; • For $p = 2$, the equation $\widetilde{E}_{d,p} \ : \ u^2 - dv^2 \equiv 1 \pmod p$ has two solutions $(1, 0),\ (1, 1)$ if $d = 0$, and two solutions $(1, 0),\ (0, 1)$ if $d = 1$.

• For $p = 3$, the equation $\widetilde{E}_{d,p} \ : \ u^2 - dv^2 \equiv 1 \pmod p$ has six solutions $(1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)$ if $d = 0$, has two solutions $(1, 0), (2, 0)$ if $d = 1$, and has four solutions $(1, 0), (2, 0), (0, 1), (0, 2)$ if $d = 2$.

Examples 3.5.

• **If** $d \in Q_p$ **and** $p \equiv 1$ (**mod** 4) **:**

1) Let $p = 17$, Consider the number of integer solutions, over $\mathbb{F}_{17}$, of the Diophantine equation

$$E \ : \ x^2 - (t^2+4)y^2 - 4tx + 4(t^2+4)y - 17 = 0,$$

for $t = 4$.

We have, $P(t) = t^2 + 4$, then $P(3) = 13 \equiv 13 \pmod{17}$, which yields $d = 13$. Its known that the problem is reduced to the Pell equation

$$\widetilde{E}_{8,11} \ : \ u^2 - 13v^2 \equiv 1 \pmod{17}.$$

As $d = 13 \in Q_{17}$, then $\#E(\mathbb{F}_{17}) = 17 - 1 = 16$. in fact,

$$\widetilde{E}_{13,17}(\mathbb{F}_{17}) = \left\{ \begin{array}{l} (0, 8), (0, 9), (1, 0), (3, 7), (3, 10), (4, 3), (4, 14), (6, 2), \\ (6, 15), (11, 2), (11, 15), (13, 3), (13, 14), (14, 7), (14, 10), \\ (16, 0) \end{array} \right\}.$$

• **If** $d \in Q_p$ **and** $p \equiv 3$ (**mod** 4) **:**

2) Let $P(t) = t^2 - 1$ and $p = 11$, then for $t = 4$, $P(t) = 15 \equiv 4 \pmod{11}$, which yields $d = 4$. We consider the number of integer solutions over $\mathbb{F}_{11}$ of the Pell equation $\widetilde{E}_{8,11} \ : \ u^2 - 4v^2 \equiv 1 \pmod{11}$. As we have $d = 4 \in Q_{13}$, then $\#E(\mathbb{F}_{13}) = 13 - 1 = 12$.

$$\widetilde{E}_{4,11}(\mathbb{F}_{11}) = \left\{ \begin{array}{l} (0, 4), (0, 9), (1, 0), (2, 2), (2, 11), (6, 5), (6, 8), (7, 5), \\ (7, 8), (11, 2), (11, 11), (12, 0) \end{array} \right\}.$$

• **If** $d \notin Q_p$ **and** $p \equiv 1$ (**mod** 4) **:**

1) Let $P(t) = t^2 - 2$ and $p = 13$, then for $t = 4$, $P(t) = 15 \equiv 2 \pmod{13}$, which yields $d = 2$. We consider the number of integer solutions over $\mathbb{F}_{13}$ of the Pell equation $\widetilde{E}_{2,13} \ : \ u^2 - 2v^2 \equiv 1 \pmod{11}$. We have

$$\left\{ \begin{array}{l} d = 2 \notin Q_{13} \\ \\ p = 13 \equiv 1 \pmod 4, \end{array} \right.$$

then $\#E(\mathbb{F}_{13}) = 13 - 1 = 12$. In fact,

$$\widetilde{E}_{2,13}(\mathbb{F}_{13}) = \left\{ \begin{array}{l} (1,0), (12,0), (3,2), (3,11), (4,1), (4,12), (8,5), (8,8), (9,1), \\ (9,12), (10,2), (10,11) \end{array} \right\}.$$

• **If** $d \notin Q_p$ **and** $p \equiv 3$ (**mod** 4) **:**

1) Let $P(t) = t^2 - t$ and $p = 31$, then for $t = 4$, $P(4) = 12 \equiv 12 \pmod{31}$, which yields $d = 12$. We consider the number of integer solutions over $\mathbb{F}_{31}$ of the Pell equation $\widetilde{E}_{12,31} : u^2 - 12v^2 \equiv 1 \pmod{31}$. We have

$$\begin{cases} d = 12 \notin Q_{31} \\ \\ p = 31 \equiv 3 \pmod 4, \end{cases}$$

then $\#E(\mathbb{F}_{31}) = 31 + 1 = 32$. In fact,

$$\widetilde{E}_{12,31}(\mathbb{F}_{31}) = \left\{ \begin{array}{l} (0, 7), (0, 24), (1, 0), (2, 15), (2, 16), (4, 3), (4, 28), (5, 8), \\ (5, 23), (7, 2), (7, 29), (10, 4), (10, 27), (11, 14), (11, 17), \\ (13, 13), (13, 18), (18, 13), (18, 18), (20, 14), (20, 17), \\ (21, 4), (21, 27), (24, 2), (24, 29), (26, 8), (26, 23), (27, 3), \\ (27, 28), (29, 15), (29, 16), (30, 0) \end{array} \right\}.$$

4. Conclusion

It is presented a study of the generalization of the quadratic Diophantine equation given by Arzu Ozkoc and Ahmet Tekcan in (Ozkoc and Tekcan, 2010). Some examples of the obtained results are considered.

Acknowledgements

We would like to thank Saäd Chandoul and Massöuda Loörayed for helpful discussions and many remarks.

References

Chandoul, A. (2011). On Polynomials Solutions of Quadratic Diophantine Equations. *Advances in Pure Mathematics, 1,* 155-159. https://doi.org/10.4236/apm.2011.14028

Chandoul, A. (2011). On quadratic Diophantine equation $x^2 - (t^2 - t)y^2 - (16t - 4)x + (16t2 - 16t)y = 0$. *International Mathematical Forum, 6*(36), 1777 - 1782.

Chandoul, A. (2011). The Pell Equation $X^2 - Dy^2 = ?k^2$. *Advances in Pure Mathematics, 01*(02), 16-22. https://doi.org/10.4236/apm.2011.12005

Chandoul, A. (2011). The Pell Equation $X^2 - Dy^2 = ?9$. *International Research Journal of Pure Algebra, 1*(1), 11-15.

Hilbert, D. (1900). Mathematische Probleme. Vortrag, gehalten auf dem Internationalen Mathematiker Kongress zu Paris 1900, Nachr. K. Ges. Wiss., G. Ottingen. *Math.-Phys.Kl*, 253-297.

Matiyasevich, Y. V. (1970). Solution of the tenth problem of Hilbert. *Mat. Lapok, 21*, 83-87.

Ozkoc, A., Tekcan, A., & Cangul, I. N. (2011). Solving some parametric quadratic Diophantine equation over Z and F_p. *Applied Mathematics and Computation, 218*(3), 703-706. https://doi.org/10.1016/j.amc.2011.03.071

Ozkoc, A., & Tekcan, A. (2010). Quadratic Diophantine Equation $x^2 - (t^2 - t)y^2 - (4t - 2)x + (4t^2 - 4t)y = 0$. *Bull. Malays. Math. Sci. Soc, 33*(2), 273-280.

Tekcan, A. (2007). The Cubic Congruence $x^3 + ax^2 + bx + c = 0$ (modp) And Binary Quadratic Forms $F(x, y) = ax^2 + bxy + cy2$.. *Ars Comb. 85*.

Tekcan A., Bizim, O., & Bayraktar, M. (2006). Solving the Pell Equation Using the Fundamental Element of the Field $\mathbb{Q}(\sqrt{\Delta})$. *Southeast Asian Bulletin of Mathematics, 30,* 355-366.

Tekcan, A. (2004). Pell Equation $x^2Dy^2 = 2, II$. *Irish Math. Soc. Bulletin, 54*, 73- 89.