International Journal of Mathematics and
Computer Science, **16**(2021), no. 4, 1435–1443

On the set of solutions of $x^2 - axy - y^2 = \pm 1$ over some finite fields

Supawadee Prugsapitak

Algebra and Applications Research Unit
Division of Computational Science
Faculty of Science
Prince of Songkla University
Hatyai, Songkhla 90110, Thailand

email: supawadee.p@psu.ac.th

(Received December 29, 2020, Revised January 6, 2021,
Accepted April 6, 2021)

Abstract

Given a finite field $\mathbb{Z}_p$ for some odd prime p, we count the number of solutions of Diophantine equations $x^2-axy-y^2 = 1$ and $x^2-axy-y^2 = -1$ over $\mathbb{Z}_p$. Their solutions are comprised of recursive sequences $\{U_n\}$ modulo p where $U_0, U_1,\ a \in \mathbb{Z}_p^\times$ and $U_{n+1} = aU_n + U_{n-1}$ for $n \geq 1$. Moreover, we give some results on the period of the sequence $\{U_n\}$ by using the number of solutions of indicated equations.

1 Introduction

In 1876, Lucas [5] proved that if x and y are consecutive Fibonacci numbers then (x, y) satisfies

$$y^2 - xy - x^2 = \pm 1$$

and the converse was proved in 1902 by Wasteels [6]. However, if we reduce these solutions modulo p for some prime p, then we can see that some solutions are not Fibonacci sequences modulo p. For example, the Fibonacci

Key words and phrases: Fibonacci, Diophantine Equation, Finite Field.
AMS (MOS) Subject Classifications: 11D09, 11B39.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

sequence modulo 11 is:

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, \ldots.$$

All solutions of $x^2 - xy - y^2 = 1$ modulo 11 are

$$(1, 0), (2, 1), (5, 3), (2, 8), (1, 10), (10, 0), (9, 10), (6, 8), (9, 3), (10, 1).$$

We can see that some solutions are pairs of consecutive Fibonacci numbers, namely $(1, 0), (2, 1), (5, 3), (2, 8)$ and $(1, 10)$ but some are not. So this motivates the author to find all solutions of the following Diophantine equations

$$x^2 - axy - y^2 = 1 \tag{1.1}$$

and

$$x^2 - axy - y^2 = -1 \tag{1.2}$$

over $\mathbb{F}_p$. These equations are studied over integers by McDaniel [7] in 1995, Keskin [2] in 2010, and Keskin and Demirturk [3] in 2010. The questions are also extended to the ring of algebraic integers of any complex quadratic number fields by Prugsapitak, Chaiya and Chaiya in 2017 [8]. However they are no relevant results on finite fields $\mathbb{F}_p$. In the present study, the author aims to compute the number of solutions of the above equations and show how solutions are partitioned. Moreover some properties of the periods of Fibonacci sequences modulo primes which were considered by Wall[10], Robinson[9] and Gupta, Rockstroh and Su [1] are presented.

2 Preliminary

Throughout the entire paper, let p be an odd prime. Then $\mathbb{F}_p$ is the finite field of order p which is also known as $\mathbb{Z}/p\mathbb{Z}$, the integers mod p. Let a be an element in $\mathbb{Z}/p\mathbb{Z}$. We first define the sets $S^p_{a,1}$ and $S^p_{a,-1}$ subsets of $(\mathbb{Z}/p\mathbb{Z})^2$ as follows:

$$S^p_{a,1} = \{(x, y) | x^2 - axy - y^2 = 1\}$$

and

$$S^p_{a,-1} = \{(x, y) | x^2 - axy - y^2 = -1\}.$$

Our first objective here is to compute the cardinality of both sets. Using the same technique as appeared in [4], we obtain the following theorem.

Theorem 2.1. *Let p be an odd prime. For $a, b \in \mathbb{Z}/p\mathbb{Z}$ and $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, the number of solutions of*

$$x^2 + axy + by^2 = k \tag{2.3}$$

over $\mathbb{Z}/p\mathbb{Z}$ is

$$N(x^2+axy+by^2 = k) = \begin{cases} 0 & \text{if} \quad p \mid (4b-a^2) \quad \text{and} \quad \left(\frac{k}{p}\right) = -1 \\ 2p & \text{if} \quad p \mid (4b-a^2) \quad \text{and} \quad \left(\frac{k}{p}\right) = 1 \\ p - \left(\frac{a^2-4b}{p}\right) & \text{if} \quad p \nmid (4b-a^2). \end{cases}$$

Proof. If the equation (2.3) holds, then $(2x + ay)^2 + (4b - a^2)y^2 = 4k$. We consider 2 cases.

Case 1: $(4b - a^2) \equiv 0 \mod p$. Then $(2x + ay)^2 = 4k$. If $(\frac{k}{p}) = -1$, then (2.3) has no solution. If $(\frac{k}{p}) = 1$, then $2x + ay \equiv \pm n \mod p$ for some n such that $n^2 = 4k$. For each k, there are two such n. Therefore for each y there are two x corresponding to y. Hence there are $2p$ solutions,

Case 2: $(4b - a^2) \not\equiv 0 \mod p$. So we let $u = 2x + ay$ and $v = y$. Then

$$\begin{aligned} N(x^2 + axy + by^2 = k) &= N(u^2 + (4b - a^2)v^2 = 4k) \\ &= \sum_{j \in \mathbb{Z}/p\mathbb{Z}} N(u^2 = 4k - j) N((4b - a^2)v^2 = j) \\ &= \sum_{j \in \mathbb{Z}/p\mathbb{Z}} N(u^2 = 4k - j) N(v^2 = (4b - a^2)^{-1} j) \end{aligned}$$

Since $N(u^2 = 4k - j) = 1 + \left(\frac{4k-j}{p}\right)$ and $N(v^2 = (4b - a^2)^{-1}j) = 1 + \left(\frac{(4b-a^2)^{-1}j}{p}\right)$, the last sum above becomes

$$p + \sum_{j \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{4k - j}{p}\right) + \sum_{j \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{(4b - a^2)^{-1} j}{p}\right) + \sum_{j \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{(4b - a^2)^{-1} j}{p}\right) \left(\frac{4k - j}{p}\right).$$

Since the first two sums are zero, we have

$$N(x^2 + axy - y^2 = k) = p + \sum_{j \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{(4b - a^2)^{-1} j}{p}\right) \left(\frac{4k - j}{p}\right)$$

and

$$\sum_{j\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{(4b-a^2)^{-1}j}{p}\right)\left(\frac{4k-j}{p}\right)=\sum_{j\in(\mathbb{Z}/p\mathbb{Z})^\times,j\neq 4k}\left(\frac{(4b-a^2)^{-1}j(4k-j)}{p}\right)$$
$$=\sum_{j\in(\mathbb{Z}/p\mathbb{Z})^\times,j\neq 4k}\left(\frac{(4b-a^2)j(4k-j)^{-1}}{p}\right)$$

Let $i=j(4k-j)^{-1}$ then $j=4ki(i+1)^{-1}$.

$$\sum_{j\in(\mathbb{Z}/p\mathbb{Z})^\times,j\neq 4k}\left(\frac{(4b-a^2)j(4k-j)^{-1}}{p}\right)=\sum_{i\in(\mathbb{Z}/p\mathbb{Z})^\times,i\neq -1}\left(\frac{(4b-a^2)i}{p}\right)$$
$$=-\left(\frac{a^2-4b}{p}\right).$$

Example 2.2. *With the notations in Theorem 2.1, if* $a=b=-1,k=1$ *and* $p=11$ *then* $N(x^2-xy-y^2=1)=10$.

We next explore the solutions of $x^2-axy-y^2=\pm 1$ which are not Fibonacci numbers and see how the sets of solutions of $x^2-axy-y^2=\pm 1$ are partitioned.

Let $U_0,U_1\in\mathbb{Z}/p\mathbb{Z}$, $a\in(\mathbb{Z}/p\mathbb{Z})^\times$ and $U_{n+1}=aU_n+U_{n-1}$ where $n\geq 1$. It is easy to see that the followings hold.

Theorem 2.3. *Let* $\{U_n\}$ *be a sequence defined as above. If* $U_1^2-aU_1U_0-U_0^2=\pm 1$ *then* $U_{2n+1}^2-aU_{2n+1}U_{2n}-U_{2n}^2=\pm 1, n\geq 0$.

Proof. Since $U_1^2-aU_1U_0-U_0^2=\pm 1$, the theorem holds for $n=0$. Assume that $U_{2n+1}^2-aU_{2n+1}U_{2n}-U_{2n}^2=\pm 1$ for some non-negative integer n. Then

$$\begin{aligned}
&U_{2n+3}^2-aU_{2n+3}U_{2n+2}-U_{2n+2}^2\\
&=\left((a^2+1)U_{2n+1}+aU_{2n}\right)^2-a\left((a^2+1)U_{2n+1}+aU_{2n}\right)(aU_{2n+1}+U_{2n})-\\
&(aU_{2n+1}+U_{2n})^2\\
&=\left((a^2+1)^2-a^2(a^2+1)-a^2\right)U_{2n+1}^2-aU_{2n+1}U_{2n}-U_{2n}^2\\
&=U_{2n+1}^2-aU_{2n+1}U_{2n}-U_{2n}^2=\pm 1.
\end{aligned}$$

This completes the proof.

Now, let $M_a = \begin{bmatrix} a^2+1 & a \\ a & 1 \end{bmatrix}$ be a matrix in $\mathbb{Z}/p\mathbb{Z}$. It is easy to see that $M \in SL(2, \mathbb{Z}/p\mathbb{Z})$.

For each $i = -1, 1$, we first prove that if $(x, y) \in S^p_{a,i}$ then $M_a \begin{bmatrix} x \\ y \end{bmatrix} \in S^p_{a,i}$.

Theorem 2.4. *For any* $i = 1, -1$ *if* $(x, y) \in S^p_{a,i}$ *then*

$$M_a \begin{bmatrix} x \\ y \end{bmatrix} \in S^p_{a,i}.$$

Proof. Let $(x, y) \in S^p_{a,i}$ and

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} a^2+1 & a \\ a & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} (a^2+1)x + ay \\ ax + y \end{bmatrix}.$$

Then

$$\begin{aligned} x_1^2 - ax_1y_1 - y_1^2 &= \big((a^2+1)x + ay\big)^2 - a((a^2+1)x + ay)(ax + y) - (ax + y)^2 \\ &= a^4x^2 + 2a^2x^2 + x^2 + 2a^3xy + 2axy + a^2y^2 - a^4x^2 - a^2x^2 \\ &\quad - a^3xy - axy - a^3xy - a^2y^2 - a^2x^2 - 2axy - y^2 \\ &= x^2 - axy - y^2. \end{aligned}$$

Since $(x, y) \in S^p_{a,i}, (x_1, y_1) \in S^p_{a,i}$. Similarly, we can show that for non-negative integer n and $i \in \{\pm 1\}$, if $(x, y) \in S^p_{a,i}$ then

$$M_a^n \begin{bmatrix} x \\ y \end{bmatrix} \in S^p_{a,i}.$$

Thus a group $G_a(p) = \langle M_a \rangle$ acts on a set $S^p_{a,i}$. Such an action induces an equivalence relation on $S^p_{a,i}$, namely

$$\{((x_1, y_1), (x_2, y_2)) \in S^p_{a,i} \times S^p_{a,i} \mid \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = M_a^k \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}, k \in \mathbb{Z}\},$$

the equivalence classes of which are the orbits of the action. The set of orbits is denoted by $S^p_{a,i}/G_a(p)$.

For any $(x_0, y_0) \in S^p_{a,i} \times S^p_{a,i}$ and for $i = 1, 2$, we denote the orbit by

$$C^p_{a,i}(x_0, y_0) = \{(x, y) \in S^p_{a,i} \times S^p_{a,i} \mid \begin{bmatrix} x \\ y \end{bmatrix} = M_a^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \quad \text{for some} \quad n \geq 0\}.$$

With the notation above, we provide some values of $S^p_{a,i}$ and $G_a(p)$ for $a = 1, 2$ and $3 \leq p \leq 29$.

a	p	$S^p_{a,i}$	$\lvert G_a(p)\rvert$	a	p	$S^p_{a,i}$	$\lvert G_a(p)\rvert$
1	3	4	4	2	3	4	4
1	5	10	10	2	5	6	6
1	7	8	8	2	7	6	3
1	11	10	5	2	11	12	12
1	13	14	14	2	13	14	14
1	17	18	18	2	19	16	8
1	19	18	9	2	19	20	20
1	23	24	24	2	23	22	11
1	29	28	7	2	29	30	10

Table 1: $S^p_{a,i}$ and $G_a(p)$ for $a = 1, 2$ and $3 \leq p \leq 29$

Next, we illustrate some examples.

Example 2.5. *The solution of* $x^2 - xy - y^2 = 1$ *over* $\mathbb{Z}/11\mathbb{Z}$.

By computation, we obtain that

$$\begin{aligned} S^{11}_{1,1} &= \{(x, y) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \mid x^2 - xy - y^2 = 1\} \\ &= \{(1, 0), (1, 10), (2, 1), (2, 8), (5, 3), (6, 8), (9, 3), (9, 10), (10, 0), (10, 1)\}. \end{aligned}$$

We now compute all orbits of the action of a group G *on a set* $S^{11}_{1,1}$. *The first orbit is*

$$C^{11}_{1,1}(1, 0) = \{(1, 0), (2, 1), (5, 3), (2, 8), (1, 10)\}.$$

We can see that each element in $C^{11}_{1,1}(1, 0)$ *is obtained from the sequence* $U_{n+1} = U_n + U_{n-1}$ *where* $U_0 = 0$ *and* $U_1 = 1$, *namely* $0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, \ldots$.

The second orbit is

$$C^{11}_{1,1}(10, 0) = \{(10, 0), (9, 10), (6, 8), (9, 3), (10, 1)\}.$$

We can see that each element in $C^{11}_{1,1}(10, 0)$ *is obtained from the sequence* $U_{n+1} = U_n + U_{n-1}$ *where* $U_0 = 0$ *and* $U_1 = 10$, *namely* $0, 10, 10, 9, 8, 6, 3, 9, 1, 10, 0, 10, \ldots$.

Thus $S^{11}_{1,1}/G_1(11) = \{C^{11}_{1,1}(1, 0), C^{11}_{1,1}(10, 0)\}$.

Example 2.6. *The solution of* $x^2 - xy - y^2 = -1$ *over* $\mathbb{Z}/11\mathbb{Z}$.

By computation, we obtain that

$$\begin{aligned} S^{11}_{1,-1} &= \{(x, y) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \mid x^2 - xy - y^2 = 1\} \\ &= \{(0, 1), (0, 10), (1, 1), (1, 9), (3, 2), (3, 6), (8, 5), (8, 9), (10, 2), (10, 10)\}. \end{aligned}$$

We now compute all orbits of the action of a group G on a set $S^{11}_{1,-1}$. The first orbit is

$$C^{11}_{1,-1}(0,1) = \{(0,1),(1,1),(3,2),(8,5),(10,2)\}.$$

We can see that each element in $C^{11}_{1,-1}(0,1)$ is obtained from the sequence $U_{n+1} = U_n + U_{n-1}$ where $U_0 = 1$ and $U_1 = 0$, namely $1,0,1,1,2,3,5,8,2,10,1,0,\ldots$. The second orbit is

$$C^{11}_{1,-1}(0,10) = \{(0,10),(10,10),(8,9),(3,6),(1,9)\}.$$

We can see that element in $C^{11}_{1,-1}(0,10)$ is obtained from the sequence $U_{n+1} = U_n + U_{n-1}$ where $U_0 = 10$ and $U_1 = 0$, namely $1001010986391100\ldots$.

Thus $S^{11}_{1,-1}/G_1(11) = \{C^{11}_{1,-1}(0,1), C^{11}_{1,-1}(0,10)\}$.

We can see from the above examples that $|S^{11}_{1,1}| = |S^{11}_{1,-1}|$ and $|S^{11}_{1,1}/G_1(11)| = |S^{11}_{1,-1}/G_1(11)|$. These follow from Theorem 2.1. Therefore the following theorem holds.

Corollary 2.7. *For any odd prime p,*

$$|S^p_{a,1}/G_1(p)| = |S^p_{a,-1}/G_1(p)| = \frac{|S^p_{a,1}|}{|G_1(p)|} = \frac{|S^p_{a,-1}|}{|G_1(p)|}.$$

Theorem 2.8. *For any non-negative integer n, $M^n_a \begin{bmatrix} U_1 \\ U_0 \end{bmatrix} = \begin{bmatrix} U_{2n+1} \\ U_{2n} \end{bmatrix}$.*

Proof. Since $M_a \begin{bmatrix} U_1 \\ U_0 \end{bmatrix} = \begin{bmatrix} U_{2(1)+1} \\ U_{2(1)} \end{bmatrix}$, the lemma holds for $n = 1$. For some $n \geq 2$, assume that $M^n \begin{bmatrix} U_1 \\ U_0 \end{bmatrix} = \begin{bmatrix} U_{2n+1} \\ U_{2n} \end{bmatrix}$ for some non-negative integer n, Then

$$\begin{aligned} M^{n+1} \begin{bmatrix} U_1 \\ U_0 \end{bmatrix} &= M \cdot M^n \begin{bmatrix} U_1 \\ U_0 \end{bmatrix} = M \cdot \begin{bmatrix} U_{2n+1} \\ U_{2n} \end{bmatrix} = \begin{bmatrix} a^2+1 & a \\ a & 1 \end{bmatrix} \cdot \begin{bmatrix} U_{2n+1} \\ U_{2n} \end{bmatrix} \\ &= \begin{bmatrix} a(aU_{2n+1} + U_{2n}) + U_{2n+1} \\ aU_{2n+1} + U_{2n} \end{bmatrix} = \begin{bmatrix} aU_{2n+2} + U_{2n+1} \\ U_{2n+2} \end{bmatrix} \\ &= \begin{bmatrix} U_{2n+3} \\ U_{2n+2} \end{bmatrix}. \end{aligned}$$

From the definition of the orbit and Theorem 2.8, we have the following corollary.

Corollary 2.9. *For any $a \in (\mathbb{Z}/p\mathbb{Z})^\times, (x,y) \in (\mathbb{Z}/p\mathbb{Z})^2$ and for any $i \in \{\pm 1\}$, we have*

$$|C_{a,i}(x,y)| = |G_a(p)|.$$

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Let $\{U_n\}$ be sequences modulo p defined previously. Let $k_a(p)$ be a period of the sequence U_n modulo p.

Corollary 2.10. *For any odd prime p and any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $k_a(p) = 2|G_a(p)|$.*

Proof. This follows from Theorem 2.8. □

Corollary 2.11. *Let $p \geq 3$ be an odd prime and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Suppose a^2+4 is not divisible by p. Then all solutions of $x^2 - axy - y^2 = 1$ over $\mathbb{Z}/p\mathbb{Z}$ are (U_{2n+1}, U_{2n}) for $n \geq 0$ and all solutions of $x^2 - axy - y^2 = -1$ over $\mathbb{Z}/p\mathbb{Z}$ are (U_{2n+2}, U_{2n+1}) for $n \geq 0$ if and only if $k_a(p) = 2\left(p - \left(\frac{a^2+4}{p}\right)\right)$.*

Proof. This follows from Theorem 2.1, Theorem 2.8 and the fact that for any $a \in \mathbb{Z}/p\mathbb{Z}^\times$, $(x,y) = (1,0)$ is a solution of $x^2 - axy - y^2 = 1$ and $(x,y) = (a,1)$ is a solution of $x^2 - axy - y^2 = -1$.

In fact, this implies that

Corollary 2.12. *Let p be an odd prime.*

1. *If a^2+4 is a non-zero quadratic residue modulo p, then $k_a(p)$ divides $2(p-1)$. In particular, $k_a(p) \leq 2(p-1)$.*
2. *If a^2+4 is a non-quadratic residue modulo p, then $k_1(p)$ divides $2(p+1)$. In particular, $k_a(p) \leq 2(p+1)$.*

This proves some parts of the result in [1], [9] and [10]. However if a^2+4 is a non-zero quadratic residue modulo p then the following holds.

Theorem 2.13 ([1]). *If p is an odd prime and a^2+4 is a non-zero quadratic residue modulo p, then $k_a(p)$ divides $p-1$. In particular, $k_a(p) \leq p-1$.*

From the above Theorem and Corollary 2.11, we can see that the following:

Corollary 2.14. *If p is an odd prime and p is congruent to 1 or 4 mod 5, then $\left|\frac{S^p_{a,1}}{G_1(p)}\right| \geq 2$.*

Acknowledgment. The author would like to thank her student, Lalita Apisornpanich, for providing some data to investigate and finish this work. We sincerely thank the referees for valuable comments.

References

[1] S. Gupta, P. Rockstroh, F. E. Su, Splitting Fields and Periods of Fibonacci Sequences Modulo Primes, Mathematics Magazine, **85**, (2012), 130–135.

[2] R. Keskin, Solutions of some quadratic Diophantine equations, Computers and Mathematics with Applications, **60**, (2010), 2225–2230.

[3] R. Keskin, B. Demirturk, Solutions of Some Diophantine Equations Using Generalized Fibonacci and Lucas Sequences, Ars Combinatoria, **111**, (2013), 161–179.

[4] S. Kongsiriwong, S. Prugsapitak, On the number of solutions of the Tarry-Escott problem of degree two and the related problem over some finite fields, Period. Math. Hung., **93**, (2014), 190–198.

[5] E. Lucas, Nouv. Corresp. Math., **2**, (1876), 201–206.

[6] M. J. Wasteels, Quelques propriété des nombres de Fibonacci, Mathesis, troisième série, tome II, (1902), 60–62.

[7] W. L. McDaniel, Diophantine Representation of Lucas Sequence, Fibonacci Quart, **33**, (1995), 59–63.

[8] S. Prugsapitak, S. Chaiya, M. Chaiya, On some Diophantine equations over complex quadratic number fields, ScienceAsia, **43,** no. 6 (2017), 383–386.

[9] D. W. Robinson, The Fibonacci matrix modulo m, Fib. Quart., **1**, (1963), 29–36.

[10] D. D. Wall, Fibonacci series modulo m, Amer. Math. Monthly, **67**, (1960), 525–532.