On the Solutions of Some Equations Over Rings of Integers Modulo the Square of a Prime

S. Jitman[*], K. Dukdokjan, and C. Wongwilai

Abstract - Algebraic equations over finite fields and over finite rings have been of interest due to their beautiful structures, usefulness in applications, and links with other mathematical objects. In this paper, the equation $X^2 - Y^2 = \alpha$ is studied over the ring of integers modulo p^2, where p is a prime number and α is an arbitrary constant. Through a matrix method, the solutions of this equation are given together with an explicit formula for the number of solutions.

Keywords : modular arithmetic equations; determinants

Mathematics Subject Classification (2020) **:** 15B33; 97H30

1 Introduction

Key problems in the study of algebraic equations deal with the solvability, solutions, number of solutions, and complexity of solving methods. Some algebraic equations over finite fields have been studied in [5] including the simple but interesting equation $X^2 - Y^2 = \alpha$. The enumeration of solutions of this equation has been completely determined. The Diophantine equation $X^2 - Y^2 = \alpha$ has been described in [3, Theorem 6.43]. Recently, the ring $\mathbb{Z}_{p^2}$ and algebraic equations over $\mathbb{Z}_{p^2}$ have become of interest due to their applications (see [1], [2] and references therein). In this article, we focus on this equation over the ring $\mathbb{Z}_{p^2}$ of integers modulo p^2, where p is a prime number. Precisely, we show that

$$X^2 - Y^2 = \alpha \tag{1}$$

over $\mathbb{Z}_{p^2}$ has a solution for all elements $\alpha \in \mathbb{Z}_{p^2}$ except $p = 2 = \alpha$. Subsequently, the solutions and the number solutions of (1) are given for all existing cases.

We first observe that finding the solutions of $X^2 - Y^2 = \alpha$ is equivalent to that of determining the matrices $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ whose determinant is

$$\alpha = a^2 - b^2 = \det\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right).$$

[*] S. Jitman was supported by the Thailand Research Fund under Research Grant RSA6280042.

Equivalently, $\det\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = \alpha$ if and only if the pair (a, b) is a solution of $X^2 - Y^2 = \alpha$. Hence, a matrix method and properties of the determinant are used in this study. Some preliminary results are recalled and proved in Section 2. The solutions and the number of solutions of $X^2 - Y^2 = \alpha$ are given in Section 3. Summary and discussion are provided in Section 4.

2 Preliminaries

For a given prime number p, denote by $\mathbb{Z}_{p^2}$ the ring of integers modulo p^2. An element $a \in \mathbb{Z}_{p^2}$ is called a *unit* or an *invertible element* if there exists an element $b \in \mathbb{Z}_{p^2}$ such that $ab = 1$. In this case, b is unique and it is called the *inverse* of a. Denote by a^{-1} the inverse of a and denote by $\mathcal{U}(\mathbb{Z}_{p^2})$ the set of units in $\mathbb{Z}_{p^2}$. A nonzero element $a \in \mathbb{Z}_{p^2}$ is called a *zero divisor* if there exists a nonzero element $b \in \mathbb{Z}_{p^2}$ such that $ab = 0$. Let $\mathcal{ZD}(\mathbb{Z}_{p^2})$ denote the set of zero divisors in $\mathbb{Z}_{p^2}$.

The following properties of $\mathbb{Z}_{p^2}$ can be derived easily. The reader refers to [4] for more details.

Lemma 2.1 *Let p be a prime. Then $\mathcal{U}(\mathbb{Z}_{p^2}) = \{a \in \mathbb{Z}_{p^2} | p \nmid a\}$ and $|\mathcal{U}(\mathbb{Z}_{p^2})| = \phi(p^2) = p(p-1)$, where ϕ is Euler's totient map.*

Lemma 2.2 *Let p be a prime. Then $\mathcal{ZD}(\mathbb{Z}_{p^2}) = \{a \in \mathbb{Z}_{p^2} \mid p|a \text{ and } a \neq 0\}$ and $|\mathcal{ZD}(\mathbb{Z}_{p^2})| = p - 1$.*

From Lemma 2.1 and Lemma 2.2, we have the following fact.

Corollary 2.3 *Let p be a prime. Then $\mathbb{Z}_{p^2} = \mathcal{U}(\mathbb{Z}_{p^2}) \cup \mathcal{ZD}(\mathbb{Z}_{p^2}) \cup \{0\}$, where the unions are disjoint.*

The following two lemmas are key to determine the solutions of (1) in Section 3.

Lemma 2.4 *Let p be a prime. Then $a \neq -a$ for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$.*

Proof. Let $a \in \mathcal{U}(\mathbb{Z}_{p^2})$. Assume that $a = -a$. Then $2a = 0$. Since $2 \neq 0$ in $\mathbb{Z}_{p^2}$, it follows that $a \in \mathcal{ZD}(\mathbb{Z}_{p^2})$, a contradiction. Therefore, $a \neq -a$ for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$. □

For $p = 2$, a solution of (1) does not need to exist (see Theorem 3.3). For each odd prime p and $\alpha \in \mathbb{Z}_{p^2}$, the existence of a solution of (1) is guaranteed by the following lemma.

Lemma 2.5 *Let p be an odd prime and $\alpha \in \mathbb{Z}_{p^2}$. Then there exist $x, y \in \mathbb{Z}_{p^2}$ such that $\alpha = x^2 - y^2$.*

Proof. We write $\alpha = a + pb$, where $0 \leq a \leq p - 1$ and $0 \leq b \leq p - 1$. Since $p \geq 3$, it follows that 2 and 4 are units in $\mathbb{Z}_{p^2}$ by Lemma 2.1. We consider the following two cases.

Case 1: $a+4^{-1} \in \mathcal{U}(\mathbb{Z}_{p^2})$. Choose $x = a+4^{-1}+2^{-1}(a+4^{-1})^{-1}bp$ and $y = a-4^{-1}$. Then

$$\begin{aligned} x^2 - y^2 &= (a+4^{-1}+2^{-1}(a+4^{-1})^{-1}bp)^2 - (a-4^{-1})^2 \\ &= a^2 + 2^{-1}a + 4^{-2} + bp - a^2 + 2^{-1}a - 4^{-2} \\ &= a + bp \\ &= \alpha. \end{aligned}$$

Case 2: $a+4^{-1} \notin \mathcal{U}(\mathbb{Z}_{p^2})$. Then $a+4^{-1} = kp$ for some $0 \leq k \leq p-1$ and $-2(4^{-1})$ is a unit in $\mathbb{Z}_{p^2}$. It follows that $a - 4^{-1} = kp - 2(4^{-1}) \in \mathcal{U}(\mathbb{Z}_{p^2})$. By setting $x = a+4^{-1}$ and $y = a - 4^{-1} + 2^{-1}(a-4^{-1})^{-1}bp$, it can be deduced that

$$\begin{aligned} x^2 - y^2 &= (a+4^{-1})^2 - (a-4^{-1}+2^{-1}(a-4^{-1})^{-1}bp)^2 \\ &= a^2 + 2^{-1}a + 4^{-2} - a^2 + 2^{-1}a - 4^{-2} + bp \\ &= a + bp \\ &= \alpha. \end{aligned}$$

As desired, for each $\alpha \in \mathbb{Z}_{p^2}$, there exist $x, y \in \mathbb{Z}_{p^2}$ such that $\alpha = x^2 - y^2$. □

The eigenvalues and eigenvectors of $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ over $\mathbb{Z}_{p^2}$ are determined in the next lemma. These results are useful in the study of the solutions of (1) in Theorem 3.3.

Lemma 2.6 *Let p be a prime and let $a, b \in \mathbb{Z}_{p^2}$. Then the following statements hold:*

1. *The eigenvalues of $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ are $a+b$ and $a-b$.*

2. *$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -1 \end{bmatrix}$ are eigenvectors of $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ corresponding to $a+b$ and $a-b$,respectively.*

Proof. From the characteristic equation

$$0 = \det\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} - \lambda I_2\right) = (\lambda - (a-b))(\lambda + (a+b)),$$

it follows that are $a+b$ and $a-b$ are the eigenvalues of $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$.

The second statement can be verified directly from 1. □

For an odd prime p, the next corollary can be deduced using direct calculation and Lemma 2.6.

Corollary 2.7 *Let p be an odd prime and let $a, b \in \mathbb{Z}_{p^2}$. Then*

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} = 2^{-1}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

For convenience, let $S_{p^2}(\alpha)$ denote the set of solutions of $X^2 - Y^2 = \alpha$ and let $s_{p^2}(\alpha) = |S_{p^2}(\alpha)|$ be the number of solutions of $X^2 - Y^2 = \alpha$. In order to apply a matrix method, let

$$C_{p^2}(\alpha) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{Z}_{p^2} \text{ and } \det\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) = \alpha \right\}.$$

As discussed above, $(a, b) \in S_{p^2}(\alpha)$ if and only if $\begin{bmatrix} a & b \\ b & a \end{bmatrix} \in C_{p^2}(\alpha)$. Hence, the number of solutions of $X^2 - Y^2 = \alpha$ is $s_{p^2}(\alpha) = |C_{p^2}(\alpha)|$.

3 Solutions of $X^2 - Y^2 = \alpha$ in

In this section, we focus on the solutions of $X^2 - Y^2 = \alpha$. The study is given in terms of matrices in $C_{p^2}(\alpha)$ separated in 3 cases where $\alpha = 0$, α is a zero divisor, and α is a unit.

First, we consider solutions of $X^2 - Y^2 = 0$.

Theorem 3.1 *Let p be a prime. Then $s_{p^2}(0) = p(3p - 2)$.*

Proof. Let $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \in C_{p^2}(0)$. Them $\det(A) = a^2 - b^2 = 0$

Case 1: $a \in \mathbb{Z}_{p^2} \setminus \mathcal{U}(\mathbb{Z}_{p^2})$. We have $a^2 = 0$ which implies that $b^2 = a^2 = 0$. Equivalently, $b \in \mathcal{ZD}(\mathbb{Z}_{p^2}) \cup \{0\}$. There are p choices of a and p choices of b by Lemma 2.1. Hence, there are p^2 choices of A.

Case 2: $a \in \mathcal{U}(\mathbb{Z}_{p^2})$. Then there are $p(p - 1)$ choices of a by Lemma 2.2. In this case, we have $b^2 = a^2$ which implies that $(b - a)(b + a) = 0$.

For $p = 2$, by inspection, the choices of (a, b) are $(1, 1), (1, 3) = (1, -1), (3, 3)$ and $(3, 1) = (3, -3)$. Consequently, we have $4 = 2p(p - 1)$ choices of A.

Assume that p is odd. Suppose that $b \neq a$ and $b \neq -a$. Since $(b - a)(b + a) = 0$, $b - a$ and $b + a$ are zero divisors which implies that $p|(b - a)$ and $p|(b + a)$ by Lemma 2.1. Then $2a = (b + a) - (b - a)$ is divisible by p. Since p is odd, it follows that $p|a$. By Lemma 2.1, a is not a unit which is a contradiction. Hence, we have $b = a$ or $b = -a$. Since $a \neq -a$ by Lemma 2.4, there are 2 choices for b. Consequently, there are $2p(p - 1)$ choices of A.

Therefore,

$$s_{p^2}(0) = |C_{p^2}(0)| = p^2 + 2p(p - 1) = p(3p - 2).$$

as desired. □

From the proof of Theorem 3.1, the solutions of $X^2 - Y^2 = 0$ can be summarized in the next corollary.

Corollary 3.2 *Let p be a prime. Then the set of solutions of $X^2 - Y^2 = 0$ is*

$$S_{p^2}(0) = \{(a, b) \mid a, b \in \mathcal{ZD}(\mathbb{Z}_{p^2}) \cup \{0\}\} \cup \{(a, \pm a) \mid a \in \mathcal{U}(\mathbb{Z}_{p^2})\}.$$

Next, we focus on the case where α is a zero divisor in $\mathbb{Z}_{p^2}$. The solutions of $X^2 - Y^2 = p$ are determined in Theorem 3.3 and extended to the case where α is an arbitrary zero divisor in Theorem 3.5.

Theorem 3.3 *Let p be a prime. Then*

$$s_{p^2}(p) = \begin{cases} 0 & \text{if } p = 2, \\ 2p(p-1) & \text{if } p \geq 3. \end{cases}$$

Proof. By inspection, $a^2 - b^2 \neq 2$ for all $a, b \in \mathbb{Z}_4$. Then $X^2 - Y^2 = 2$ has no solutions in $\mathbb{Z}_4$ which implies that $s_4(2) = 0$.

Assume that $p \geq 3$. In this case, 2 is a unit in $\mathbb{Z}_{p^2}$. Let

$$\mathcal{S}_p = \left\{ \begin{bmatrix} x & 0 \\ 0 & px^{-1} \end{bmatrix}, \begin{bmatrix} px^{-1} & 0 \\ 0 & x \end{bmatrix} \middle| x \in \mathcal{U}(\mathbb{Z}_{p^2}) \right\}.$$

Using the decomposition in Corollary 2.7, let $f : \mathcal{S}_p \to C_{p^2}(p)$ be the map defined by

$$\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} \mapsto 2^{-1} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = 2^{-1} \begin{bmatrix} r+s & s-r \\ s-r & r+s \end{bmatrix}.$$

Let $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \in C_{p^2}(p)$. Then $p = \det(A) = a^2 - b^2 = (a-b)(a+b)$ which implies that $a \neq b$ and $a \neq -b$.

Case 1: $a - b \in \mathcal{U}(\mathbb{Z}_{p^2})$. Choose $r = a - b$ and $s = p(a-b)^{-1} = a + b$. Then

$$\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} = \begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix} = \begin{bmatrix} a-b & 0 \\ 0 & p(a-b)^{-1} \end{bmatrix} \in \mathcal{S}_p$$

and

$$\begin{aligned} f\left(\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}\right) &= f\left(\begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix}\right) \\ &= 2^{-1} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \\ &= 2^{-1} \begin{bmatrix} 2a & 2b \\ 2b & 2a \end{bmatrix} \\ &= A. \end{aligned}$$

Case 2: $a - b \notin \mathcal{U}(\mathbb{Z}_{p^2})$. Then $a - b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$. Since $(a-b)(a+b) = p$, it follows that $a + b \in \mathcal{U}(\mathbb{Z}_{p^2})$. Choose $s = a + b$ and $r = p(a+b)^{-1} = a - b$. We have

$$\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} = \begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix} = \begin{bmatrix} p(a+b)^{-1} & 0 \\ 0 & a+b \end{bmatrix} \in \mathcal{S}_p$$

and

$$\begin{aligned} f\left(\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}\right) &= f\left(\begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix}\right) \\ &= 2^{-1} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} a-b & 0 \\ 0 & a+b \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ b & a \end{bmatrix} \\ &= A. \end{aligned}$$

Hence, f is a surjective map.

Since $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ are non-singular and 2 is invertible, the map f is injective. Therefore, f is a bijection which implies that

$$s_{p^2}(p) = |C_{p^2}(p)| = |\mathcal{S}_p| = 2\,|\mathcal{U}(\mathbb{Z}_{p^2})| = 2p(p-1)$$

as desired. □

From the proof of Theorem 3.3, the solutions of $X^2 - Y^2 = p$ are summarized as follows.

Corollary 3.4 *Let p be a prime. Then $S_4(2) = \emptyset$ and*

$$S_{p^2}(p) = \{2^{-1}(a + pa^{-1}, pa^{-1} - a), 2^{-1}(a + pa^{-1}, a - pa^{-1}) \mid a \in \mathcal{U}(\mathbb{Z}_{p^2})\ \}$$

for all odd primes p.

For $p = 2$, 2 is the only zero divisor in $\mathbb{Z}_4$ and $s_4(2) = 0$ is determined in Theorem 3.3. In the following theorem, we focus on $s_{p^2}(\alpha)$ for all $p \geq 3$ and for all zero divisors α in $\mathbb{Z}_{p^2}$.

Theorem 3.5 *Let $p \geq 3$ be a prime. Then $s_{p^2}(\alpha) = 2p(p-1)$ for all $\alpha \in \mathcal{ZD}(\mathbb{Z}_{p^2})$.*

Proof. Let $\alpha \in \mathcal{ZD}(\mathbb{Z}_{p^2})$. Then $\alpha = kp$ for some $0 < k < p$. By Lemma 2.5, there exist $x, y \in \mathbb{Z}_{p^2}$ such that $x^2 - y^2 = k \in \mathcal{U}(\mathbb{Z}_{p^2})$. Let $g : C_{p^2}(p) \to C_{p^2}(kp)$ be a map defined by

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \mapsto \begin{bmatrix} x & y \\ y & x \end{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

Let $A = B \in C_{p^2}(p)$ be such that $g(A) = g(B)$. Then $\begin{bmatrix} x & y \\ y & x \end{bmatrix} A = \begin{bmatrix} x & y \\ y & x \end{bmatrix} B$. Since $\begin{bmatrix} x & y \\ y & x \end{bmatrix}$ is invertible, we have $A = B$ which implies that g is injective.

Let $A = \begin{bmatrix} c & d \\ d & c \end{bmatrix} \in C_{p^2}(kp)$. Then $\det(A) = c^2 - d^2 = kp$. Choose

$$B = \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix}.$$

Then

$$\det(B) = \frac{1}{(x^2 - y^2)^2}(x^2 - y^2)(c^2 - d^2) = \frac{1}{k^2}(k)(kp) = p$$

which implies that

$$B = \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \frac{1}{x^2 - y^2} \begin{bmatrix} xc - yd & dx - yc \\ dx - yc & xc - yd \end{bmatrix} \in C_{p^2}(p)$$

and

$$g(B) = \begin{bmatrix} x & y \\ y & x \end{bmatrix} \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ d & c \end{bmatrix} = A.$$

It follows that g is a surjective map.

Hence, g is a bijection and $s_{p^2}(\alpha) = |C_{p^2}(kp)| = |C_{p^2}(p)| = 2p(p-1)$. □

Based on the proof of Theorem 3.5, for each zero divisor α in $\mathbb{Z}_{p^2}$, the solutions of $X^2 - Y^2 = \alpha$ are given in the next corollary.

Corollary 3.6 *Let $p \geq 3$ be a prime and let α be a zero divisor in $\mathbb{Z}_{p^2}$. Then*

$$S_{p^2}(\alpha) = \left\{ 2^{-1}(a + pa^{-1}, pa^{-1} - a) \begin{bmatrix} x & y \\ y & x \end{bmatrix}, \right.$$
$$\left. 2^{-1}(a + pa^{-1}, a - pa^{-1}) \begin{bmatrix} x & y \\ y & x \end{bmatrix} \middle| a \in \mathcal{U}(\mathbb{Z}_{p^2}) \right\},$$

where x and y are elements in $\mathbb{Z}_{p^2}$ such that $(x^2 - y^2)p = \alpha$ determined in Lemma 2.5.

Finally, we focus on the solutions of $X^2 - Y^2 = \alpha$, where α is a unit in $\mathbb{Z}_{p^2}$. We begin with $\alpha = 1$ in Theorem 3.7 and extend to an arbitrary unit in Theorem 3.9.

Theorem 3.7 *Let p be a prime. Then*

$$s_{p^2}(1) = \begin{cases} 4 & \text{if } p = 2, \\ p(p-1) & \text{if } p \geq 3. \end{cases}$$

Proof. By inspection, we have that $(1,0), (1,2), (3,0)$, and $(3,2)$ are the solutions of $X^2 - Y^2 = 1$ over $\mathbb{Z}_4$.

Assume that $p \geq 3$. In this case, 2 is a unit in $\mathbb{Z}_{p^2}$. Let

$$\mathcal{T}_p = \left\{ \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \middle| x \in \mathcal{U}(\mathbb{Z}_{p^2}) \right\}$$

and let $f : \mathcal{T}_p \to C_{p^2}(1)$ be the map defined by

$$\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \mapsto 2^{-1} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = 2^{-1} \begin{bmatrix} x + x^{-1} & x^{-1} - x \\ x^{-1} - x & x + x^{-1} \end{bmatrix}.$$

Let $A, B \in \mathcal{T}_p$ be such that $f(A) = f(B)$. Since 2 is a unit and $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ are non-singular, we have $A = B$ which implies that f is an injective map.

Let $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \in C_{p^2}(1)$. Then $1 = \det(A) = a^2 - b^2 = (a-b)(a+b)$. Let $x = a - b$. Then $x \in \mathcal{U}(\mathbb{Z}_{p^2})$ and $B = \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \in \mathcal{T}_p$. It follows that

$$f(B) = 2^{-1} \begin{bmatrix} a - b + a + b & a + b - a + b \\ a + b - a + b & a - b + a + b \end{bmatrix} = 2^{-1} \begin{bmatrix} 2a & 2b \\ 2b & 2a \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix} = A.$$

Hence, f is surjective.

Consequently, f is a bijection and

$$s_{p^2}(1) = |C_{p^2}(1)| = |\mathcal{T}_p| = |\mathcal{U}(\mathbb{Z}_{p^2})| = p(p-1)$$

which implies that

$$s_{p^2}(1) = \begin{cases} 4 & \text{if } p = 2, \\ p(p-1) & \text{if } p \geq 3 \end{cases}$$

as required. □

The solutions of $X^2 - Y^2 = 1$ are given in the following corollary.

Corollary 3.8 *Let p be a prime. Then*

$$S_4(1) = \{(1,0), (1,2), (3,0), (3,2)\}$$

and

$$S_{p^2}(1) = \{2^{-1}(a + a^{-1}, a - a^{-1}) \mid a \in \mathcal{U}(\mathbb{Z}_{p^2})\}$$

for all primes $p \geq 3$.

Theorem 3.7 is now extended to cover the case where α is an arbitrary unit in $\mathbb{Z}_{p^2}$.

Theorem 3.9 *Let p be a prime. Then*

$$s_{p^2}(\alpha) = \begin{cases} 4 & \textit{if } p = 2, \\ p(p-1) & \textit{if } p \geq 3 \end{cases}$$

for all $\alpha \in \mathcal{U}(\mathbb{Z}_{p^2})$.

Proof. Let $\alpha \in \mathcal{U}(\mathbb{Z}_{p^2})$. For $p = 2$, we have $u \in \{1, 3\}$. From Theorem 3.7, we have $s_{p^2}(1) = 4$. By inspection, the solutions of $X^2 - Y^2 = 3$ are $(0,1), (0,3), (2,1)$, and $(2,3)$ which implies that $s_{p^2}(3) = 4$.

Next, assume that $p \geq 3$. By Lemma 2.5, there exist $x, y \in \mathbb{Z}_{p^2}$ such that $\alpha = x^2 - y^2$. Let $g : C_{p^2}(1) \to C_{p^2}(\alpha)$ be the map defined by

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \mapsto \begin{bmatrix} x & y \\ y & x \end{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

Let $A = B \in C_{p^2}(1)$ be such that $g(A) = g(B)$. Then

$$\begin{bmatrix} x & y \\ y & x \end{bmatrix} A = \begin{bmatrix} x & y \\ y & x \end{bmatrix} B.$$

Since $\begin{bmatrix} x & y \\ y & x \end{bmatrix}$ is non-singular, we have $A = B$ which implies that g is injective.

Let $A = \begin{bmatrix} c & d \\ d & c \end{bmatrix} \in C_{p^2}(\alpha)$. Then $\det(A) = c^2 - d^2 = \alpha$. Choose

$$B = \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix}.$$

Then

$$\det(B) = \frac{1}{(x^2 - y^2)^2}(x^2 - y^2)(c^2 - d^2) = \frac{1}{u^2}(u)^2 = 1$$

and

$$B = \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \frac{1}{x^2 - y^2} \begin{bmatrix} xc - yd & dx - yc \\ dx - yc & xc - yd \end{bmatrix} \in C_{p^2}(1).$$

It can be concluded that

$$g(B) = \begin{bmatrix} x & y \\ y & x \end{bmatrix} \frac{1}{x^2 - y^2} \begin{bmatrix} x & -y \\ -y & x \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ d & c \end{bmatrix} = A.$$

Thus, g is surjective.

Consequently, g is a bijection and $s_{p^2}(\alpha) = |C_{p^2}(\alpha)| = |C_{p^2}(1)| = s_{p^2}(1)$. By Theorem 3.7, we therefore have

$$s_{p^2}(\alpha) = s_{p^2}(1) = \begin{cases} 4 & \text{if } p = 2 \\ p(p-1) & \text{if } p \geq 3 \end{cases}$$

for all $\alpha \in \mathcal{U}(\mathbb{Z}_{p^2})$ □

Corollary 3.10 *Let p be a prime and let $\alpha \in \mathcal{U}(\mathbb{Z}_{p^2})$. Then*

$$S_4(1) = \{(1,0),(1,2),(3,0),(3,2)\}, S_4(3) = \{(0,1),(0,3),(2,1),(2,3)\},$$

and

$$S_{p^2}(\alpha) = \{2^{-1}(a + a^{-1}, a - a^{-1}) \begin{bmatrix} x & y \\ y & x \end{bmatrix} \mid a \in \mathcal{U}(\mathbb{Z}_{p^2})\}$$

for all primes $p \geq 3$, where x and y are defined in Lemma 2.5.

4 Conclusions

The solutions of $X^2 - Y^2 = \alpha$ and their enumeration have been completely determined over the ring $\mathbb{Z}_{p^2}$ through a matrix method. It would be interesting to extend the study to the ring of integers modulo p^k or the ring of integers modulo m, where p is a prime and $k > 2$ and $m \geq 2$ are integers.

Acknowledgments

The authors would like to thank Trairat Jantaramas for useful discussions. We would also like to thank the referee and the editor for their useful and insightful comments.

References

[1] J.M.P. Balmaceda, R.A.L. Betty, F.R. Nemenzo, Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$. *Discrete Math.*, **308** (2020), 2984–3002.

[2] W. Choi, Y.H. Park, Self-dual codes over $\mathbb{Z}_{p^2}$ of small lengths. *Korean J. Math.*, **25** (2017), 379–388.

[3] O. Cira, F. Smarandache, *Solving Diophantine Equations*, Europa, 2015.

[4] D. Dummit, R. Foote, *Abstract Algebra*, Wiley: New York , USA, 2003.

[5] A. Weil, Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, **55** (1949), 497–508.

Somphong Jitman
Department of Mathematics
Faculty of Science, Silpakorn University
Nakhon Pathom 73000, Thailand
E-mail: `jitman_s@silpakorn.edu`

Khanittha Dukdokjan
Department of Mathematics
Faculty of Science, Silpakorn University
Nakhon Pathom 73000, Thailand
E-mail: `dukdokjan.k@gmail.com`

Chanakan Wongwilai
Department of Mathematics
Faculty of Science, Silpakorn University
Nakhon Pathom 73000, Thailand
E-mail: `aom.chanakanwong@gmail.com`

Received: September 18, 2020 **Accepted**: March 4, 2021
Communicated by Bruce Landman