Menemui Matematik (Discovering Mathematics)
Vol. 41, No. 1: 34 - 45 (2019)

Exponential Sums Associated with Quartic Polynomial

Yap H. K.[1], Sapar S. H.[2] and Mohd Atan K. A.[3]

[1,2,3]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
[1]yaphongkeat@yahoo.com, [2]sitihas@upm.edu.my, [3]kamelariffin48@gmail.com

ABSTRACT

Let $f(x,y)$ be a polynomial in $Z_p[x,y]$ and p be a prime. For $\alpha > 1$, the exponential sums associated with f modulo a prime p^α is defined as $S(f;q) = \sum e^{\frac{2\pi i f(x)}{q}}$, where the sum is taken over a complete set of residues modulo p^α. It has been shown that the exponential sums is depends on the cardinality of the set of solutions to the congruence equation associated with the quartic polynomial $f(x,y)$. The objective of this research is to estimate the exponential sums for quartic polynomial at any point $(x - x_0, y - y_0)$ restricted to some conditions. p-adic methods and Newton polyhedron technique is used to estimate the p-adic sizes of common zeros of partial derivative polynomials by constructing and analyzing the indicator diagram. The information of p-adic sizes of common zeros that obtained is applied to estimate the cardinality of the set $N(g,h;p^\alpha)$. The result of the cardinality is then used to estimate the exponential sums of the polynomial.

Keywords: p-adic sizes; Newton polyhedron; Cardinality; Exponential sums

INTRODUCTION

We use the notation of Z_p as the ring of p-adic integers, Ω_p is the completion of the algebraic closure of Q_p the field of rational p-adic numbers and $ord_p x$ as the highest power of p which divides x. Research on finding the best possible approach to estimation of the exponential sums has become one of the main subjects in number theory problem. Loxton and Vaughn (1985) are among the researchers who investigate this problem. They found that estimation of $S(f;q)$ depend on values of $|V|$, the number of common zeros of partial derivatives of f with respect to x modulo q. Since then, Mohd Atan (1986) started to investigate more on the explicit estimation of $S(f;q)$ by using lower degree polynomials, hence introduced Newton polyhedron technique to find the p-adic sizes of common zeros. Indicator diagram is constructed and being analysed. Then, Mohd Atan and Abdullah (1993) considered a polynomial of cubic form and obtained the p-adic order for the root (ξ,η) of this polynomial. After that, Chan (1997) worked on a polynomial of quartic form while Sapar and Mohd Atan (2002) estimate the cardinality of the sets of solutions in the cases where overlapping occurs at vertices of two segment on the indicator diagram associated to second and third degree polynomials. Sapar and Mohd Atan (2009) and Sapar et.al (2014) used the Newton polyhedron technique to estimate the p-adic sizes of the polynomials under considerations. In 2011, Yap et. al concentrating of finding the cardinality of the set of solution associated to a polynomial of cubic form.

p-ADIC ORDERS OF ZEROS OF A POLYNOMIALS

In this section, we focus on finding the p-adic sizes of common zeros of polynomials associated with quartic polynomial restricted with conditions of $ord_p ac^2 > ord_p b^3$. We need the following definitions and theorem developed by Mohd Atan (1986).

Definition 1: Let $f(x,y) = \sum a_{ij}x^i y^j$ be a polynomial of degree n in $\Omega_p[x,y]$. By mapping the terms $T_{ij} = a_{ij}x^i y^j$ of $f(x,y)$ to the points $P_{ij} = a_{ij}x^i y^j$ in the three-dimensional Euclidean space R^3. The set of points P_{ij} is defined as the Newton diagram of $f(x,y)$.

Definition 2 (*Newton Polyhedron*) : Let $f(x,y) = \sum a_{ij}x^i y^j$ be a polynomial of degree n in $\Omega_p[x,y]$. By mapping the terms $T_{ij} = a_{ij}x^i y^j$ of $f(x,y)$ to the points $P_{ij} = a_{ij}x^i y^j$ in the Euclidean space, the Newton polyhedron of $f(x,y)$ is defined to be the lower convex hull of the set S of points P_{ij}, $0 \leq i,j \leq n$. It is the highest convex connected surface which passes through or below the points in S. If $a_{ij} = 0$ for some (i,j) then $ord_p a_{ij} = \infty$.

Definition 3 (*Indicator Diagram*) *:* The set of lines associated with the Newton polyhedron, denoted by N_f. Let $(\mu_i, \lambda_i, 1)$ be the normalized upward-pointing normals to the faces F_i of N_f, of a polynomial $f(x,y)$ in $\Omega_p[x,y]$. The point $(\mu_i, \lambda_i, 1)$ is mapping to the point (μ_i, λ_i) in the $x - y$ plane. If F_r and F_s are adjacent faces in N_f, sharing a common edge, we construct the straight line joining (μ_r, λ_r) and (μ_s, λ_s). If F_r shares a common edges with a vertical face F say $\alpha x + \beta y = \gamma$ in N_f, we construct the straight line segment joining (μ_r, λ_r) and the appropriate point at infinity that corresponds to the normal F, that is the segment along a line with a slope $-\alpha/\beta$.

Theorem 1: Let p be a prime. Suppose f and g are polynomials in $\mathbb{Z}_p[x,y]$. Let (μ,λ) be a point of intersection of the indicator diagrams associated with f and g at the vertices or simple points of intersections. Then, there are ξ and η in Ω_p^2 satisfying $f(\xi,\eta) = g(\xi,\eta) = 0$ and $ord_p\xi = \mu_1, ord_p\eta = \mu_2$.

p-ADIC ORDERS OF COMMON ZEROS IN THE NEIGHBOURHOOD OF (x_0, y_0) WITH THE CONDITION $ord_p ac^2 > ord_p b^3$

In this section, we will estimate *p*-adic orders of common zeros of partial derivative polynomials associated with a quartic polynomial of the form $f(x,y) = ax^4 + bx^3y + cxy^3 + dy^4 + rx + sy + t$ under the condition $ord_p ac^2 > ord_p b^3$. We first prove the following lemmas as we will apply them in the proof of theorem.

In the following lemma, show that the partial derivative polynomials associated with $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$ can be rewritten into a simpler form by the transformation method of Sapar and Mohd Atan (2009)

Lemma 1:Let $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$ be a polynomial in $Z_p[x,y]$ with $p > 3$. Let λ be a constant such that $\frac{2b+3\lambda c}{4a} - 3\left(\frac{b\lambda}{6a}\right)^2 = 0$ and $\frac{c+4\lambda d}{4a} - \left(\frac{b\lambda}{6a}\right)^3 = 0$. Then $(f_x + \lambda f_y)(x,y) = 4a\left[x + \left(\frac{b\lambda}{6a}\right)y\right]^3 + r + \lambda s$.

Proof:

From $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$, we have

$f_x(x,y) = 4ax^3 + 2bxy^2 + cy^3 + r$ and $f_y(x,y) = 2bx^2y + 3cxy^2 + 4dy^3 + s$.

Thus,

$$\frac{(f_x + \lambda f_y)(x,y)}{4a} = x^3 + 3\left(\frac{b\lambda}{6a}\right)x^2y + 3\left(\frac{b\lambda}{6a}\right)^2 xy^2 + \left(\frac{b\lambda}{6a}\right)^3 y^3 + \frac{r+\lambda s}{4a}$$
$$+\left[\frac{2b+3\lambda c}{4a} - 3\left(\frac{b\lambda}{6a}\right)^2\right]xy^2 + \left[\frac{c+4\lambda d}{4a} - \left(\frac{b\lambda}{6a}\right)^3\right]y^3.$$

Since $\frac{2b+3\lambda c}{4a} - 3\left(\frac{b\lambda}{6a}\right)^2 = 0$ and $\frac{c+4\lambda d}{4a} - \left(\frac{b\lambda}{6a}\right)^3 = 0$, we have

$$(f_x + \lambda f_y)(x,y) = 4a\left[x + \left(\frac{b\lambda}{6a}\right)y\right]^3 + r + \lambda s.$$

□

Throughout the ensuing discussion $p(x)$ and $q(x)$ will denote polynomials in $Z_p[x]$ of the form $p(x) = b^3x^3 - 216a^2dx - 54a^2c$ and $q(x) = b^2x^2 - 9acx - 6ab$ respectively. Lemma below gives the condition that ensure the existence of common zeros for $p(x)$ and $q(x)$.

Lemma 2 :Let $p(x) = b^3x^3 - 216a^2dx - 54a^2c$ and $q(x) = b^2x^2 - 9acx - 6ab$ be polynomials in $Z_p[x,y]$ with $p > 3$. If $2b^3 + 27ac^2 = 72abd$, then $q(x)|p(x)$.

Proof:

From $p(x) = b^3x^3 - 216a^2dx - 54a^2c$, we rewrite this in the following form

$$p(x) = \left(bx + \frac{9ac}{b}\right)q(x) + \frac{3a}{b}(2b^3 - 72abd + 27ac^2)x.$$

Since $2b^3 + 27ac^2 = 72abd$, then

$$p(x) = \left(bx + \frac{9ac}{b}\right)q(x).$$

Therefore, $q(x)|p(x)$.

□

From the lemma above, $q(x)$ is the factor of $p(x)$. This implies that zeros of $q(x)$ are also zeros of $p(x)$. In other words, there exists at most two common zeros for $p(x)$ and $q(x)$.

The lemma below gives the p-adic orders of common zeros of $p(x)$ and $q(x)$ under the condition $ord_p ac^2 > ord_p b^3$.

Lemma 3: Let $p > 3$ be a prime and a, b, c and d in Z_p. Suppose λ is a common root of $p(x) = b^3x^3 - 216a^2dx - 54a^2c$ and $q(x) = b^2x^2 - 9acx - 6ab$. If $ord_p ac^2 > ord_p b^3$, then $ord_p\lambda = \frac{1}{2} ord_p \frac{a}{b}$.

Proof:

We have $p(x) = b^3x^3 - 216a^2dx - 54a^2c$ and $q(x) = b^2x^2 - 9acx - 6ab$. Now the discriminant, $D = 81a^2c^2 + 24ab^3$ is clearly not zero. Hence $p(x)$ and $q(x)$ have two distinct common roots, λ_1 and λ_2. The common roots of $q(x)$ are given by

$$\lambda = \frac{9ac \pm \sqrt{(9ac)^2 + 24(b^2)(ab)}}{2b^2}.$$

It follows that,

$$ord_p\lambda = ord_p \frac{9ac \pm \sqrt{(9ac)^2 + 24(b^2)(ab)}}{2b^2}$$

$$= \min\left\{ord_p 9ac, \frac{1}{2}\min\{ord_p(9ac)^2, ord_p 24(b^2)(ab)\}\right\} - ord_p b^2.$$

Since $ord_p ac^2 > ord_p b^3$, then

$$ord_p\lambda = \frac{1}{2} ord_p(b^2)(ab) - ord_p b^2$$

$$= \frac{1}{2} ord_p a - \frac{1}{2} ord_p b$$

That is, $ord_p\lambda = \frac{1}{2} ord_p \frac{a}{b}$.

□

Lemma below shows the p-adic orders of common zeros of $f(x,y) = x^3 + ax^2 + bx + c$ and $g(x,y) = y^3 + ry^2 + sy + t$ can be obtained from the combination of indicator diagrams associated with the Newton polyhedra of $f(x,y)$ and $g(x,y)$.

Lemma 4: Suppose $f(x,y) = x^3 + ax^2 + bx + c$ and $g(x,y) = y^3 + ry^2 + sy + t$ are polynomials in $Z_p[x,y]$. Let (μ,λ) be a point of intersection of the indicator diagrams associated with the Newton polyhedra of $f(x,y)$ and $g(x,y)$. Then, there exists (α,β) in ${\Omega_p}^2$ such that $f(\alpha,\beta) = 0$, $g(\alpha,\beta) = 0$, $ord_p\alpha = \mu = \frac{1}{2} ord_p c$ and $ord_p\beta = \lambda = \frac{1}{2} ord_p t$.

Proof:

We have $f(x,y) = x^3 + ax^2 + bx + c$ and $g(x,y) = y^3 + ry^2 + sy + t$. We construct the indicator diagrams associated with the Newton polyhedra of $f(x,y)$ and $g(x,y)$ by using Definitions 2 and 3. The combination of indicator diagrams for both $f(x,y)$ and $g(x,y)$ is as in the following figure.

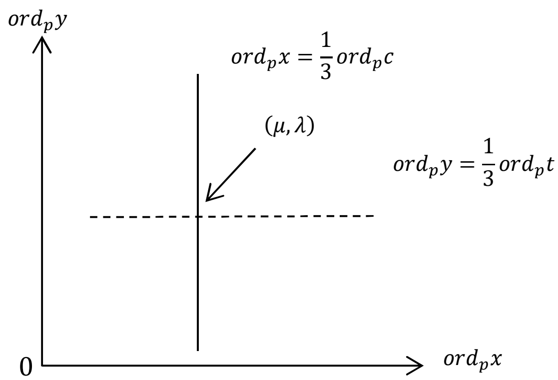

Figure 1: The combination of indicator diagrams associated with $f(x,y) = x^3 + ax^2 + bx + c$(in solid lines) and $g(x,y) = y^3 + ry^2 + sy + t$. (in dash lines)

We see that there is an intersection point (μ, λ) such that

$$\mu = \tfrac{1}{3} ord_p c \text{ and } \lambda = \tfrac{1}{3} ord_p t.$$

By a theorem of Mohd Atan (1986), there exists (α, β) in $\Omega_p{}^2$ such that $f(\alpha, \beta) = 0$, $g(\alpha, \beta) = 0$ and

$$ord_p \alpha = \mu = \tfrac{1}{3} ord_p c \text{ and } ord_p \beta = \lambda = \tfrac{1}{3} ord_p t \ .$$

□

In the lemma below, we solve $u = x + \tau_1 y$ and $v = x + \tau_2 y$ simultaneously and then obtain $ord_p x$ and $ord_p y$ respectively in terms of u, v, τ_1 and τ_2.

Lemma 5: Suppose $p > 3$ be a prime. Let τ_1, τ_2 be constants and (x, y) be a point in Ω_p^2 and $u = x + \tau_1 y$, $v = x + \tau_2 y$. Then $ord_p x = ord_p(\tau_1 v - \tau_2 u) - ord_p(\tau_1 - \tau_2)$ and $ord_p y = ord_p(u - v) - ord_p(\tau_1 - \tau_2)$.

Proof:

Let $$u = x + \tau_1 y \quad (1)$$

and $$v = x + \tau_2 y. \quad (2)$$

Subtracting (2) from (1), we obtain

$$y = \frac{u - v}{\tau_1 - \tau_2}. \quad (3)$$

Multiplying (1) by τ_2 and (2) by τ_1, then solving simultaneously will be obtained

$$x = \frac{\tau_1 v - \tau_2 u}{\tau_1 - \tau_2}.$$

It follows that

$$ord_p x = ord_p(\tau_1 v - \tau_2 u) - ord_p(\tau_1 - \tau_2).$$

Also from (3), $$ord_p y = ord_p(u - v) - ord_p(\tau_1 - \tau_2).$$

□

The following assertion gives the p-adic orders of common zeros of partial derivative polynomials associated with a quartic polynomial of the form $f(x,y) = ax^4 + bx^3 y + cxy^3 + dy^4 + rx + sy + t$. The condition $ord_p ac^2 > ord_p b^3$ applied in the following assertion influences the p-

adic orders of common zeros of partial derivative polynomials associated with the polynomial considered.

Theorem 2
Let $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$ be a polynomial in $Z_p[x,y]$ with $p > 3$. Let $\alpha > 0$ and $\delta = \max\{ord_p a, ord_p b, ord_p c, ord_p d\}$. Suppose $(x_0, y_0) \in \Omega_p^2$, $ord_p ac^2 > ord_p b^3$ and $2b^3 + 27ac^2 = 72abd$. If $ord_p f_x(x_0,y_0), ord_p f_y(x_0,y_0) \geq \alpha > \delta$, then there exists $(\xi,\eta) \in \Omega_p^2$ such that $f_x(\xi,\eta) = 0$, $f_y(\xi,\eta) = 0$ and $ord_p(\xi - x_0) \geq \frac{1}{3}(\alpha - \delta)$, $ord_p(\eta - y_0) \geq \frac{1}{3}(\alpha - \delta)$ or $ord_p(\eta - y_0) > \frac{1}{3}(\alpha - 2\delta)$.

Proof:
Given $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$, we have from Lemma 1,

$$(f_x + \lambda f_y)(x,y) = 4a\left[x + \left(\frac{b\lambda}{6a}\right)y\right]^3 + r + \lambda s$$

where λ is a constant. Let $X = x - x_0$ and $Y = y - y_0$. Then

$$(f_x + \lambda f_y)(X + x_0, Y + y_0) = 4a\left[(X + x_0) + \left(\frac{b\lambda}{6a}\right)(Y + y_0)\right]^3 + r + \lambda s \tag{4}$$

if

$$\frac{2b + 3\lambda c}{4a} - 3\left(\frac{b\lambda}{6a}\right)^2 = 0 \tag{5}$$

and

$$\frac{c + 4\lambda d}{4a} - \left(\frac{b\lambda}{6a}\right)^3 = 0. \tag{6}$$

By expanding equations (5) and (6), we obtain $p(\lambda) = b^3\lambda^3 - 216a^2d\lambda - 54a^2c = 0$ and $q(\lambda) = b^2\lambda^2 - 9ac\lambda - 6ab = 0$ respectively. Since $2b^3 + 27ac^2 = 72abd$, by Lemma 2, there exists at most two common roots, λ of the polynomials. Now the discriminant, $D = 81a^2c^2 + 24ab^3$ of $q(\lambda)$ is clearly not zero since if $D = 0$ then $ord_p ac^2 = ord_p b^3$ is contradicting with the condition $ord_p ac^2 > ord_p b^3$. Hence $p(\lambda)$ and $q(\lambda)$ have two distinct common roots, λ_1 and λ_2.

Let

$$U = X + \frac{b\lambda_1}{6a}Y,\ u_0 = x_0 + \frac{b\lambda_1}{6a}y_0 \tag{7}$$

$$V = X + \frac{b\lambda_2}{6a}Y,\ v_0 = x_0 + \frac{b\lambda_2}{6a}y_0. \tag{8}$$

By substituting U and V into (4), we obtain polynomials in (U,V) as follows:

$$F(U,V) = 4a(U + u_0)^3 + r + \lambda_1 s \tag{9}$$

and

$$G(U,V) = 4a(V + v_0)^3 + r + \lambda_2 s. \tag{10}$$

From (9) and (10), we obtain

$$F(U,V) = 4a[U^3 + 3u_0U^2 + 3{u_0}^2U] + F_0$$
$$G(U,V) = 4a[V^3 + 3v_0V^2 + 3{v_0}^2V] + G_0$$

where $F_0 = f_x(x_0,y_0) + \lambda_1 f_y(x_0,y_0)$ and $G_0 = f_x(x_0,y_0) + \lambda_2 f_y(x_0,y_0)$.

By Lemma 4, there exists $(\widehat{U}, \widehat{V})$ in ${\Omega_p}^2$ such that $F(\widehat{U}, \widehat{V}) = 0$, $G(\widehat{U}, \widehat{V}) = 0$ where

$$ord_p\widehat{U} = \mu' = \frac{1}{3}ord_p\frac{F_0}{4a} \text{ and } ord_p\widehat{V} = \lambda' = \frac{1}{3}ord_p\frac{G_0}{4a}.$$

By equations (7) and (8), there exists $(\hat{X}, \hat{Y})$ such that

$$\widehat{U} = \hat{X} + \gamma_1\hat{Y} \quad (11)$$

$$\widehat{V} = \hat{X} + \gamma_2\hat{Y}. \quad (12)$$

where $\gamma_i = \frac{b\lambda_i}{6a}$ for $i = 1,2$.

By Lemma 5, we have

$$ord_p\hat{X} = ord_p(\gamma_1\widehat{V} - \gamma_2\widehat{U}) - ord_p(\gamma_1 - \gamma_2) \quad (13)$$

and

$$ord_p\hat{Y} = ord_p(\widehat{U} - \widehat{V}) - ord_p(\gamma_1 - \gamma_2). \quad (14)$$

In equation (13), there are four cases to be considered as below.
Suppose $\min\{ord_p\gamma_1\widehat{V}, ord_p\gamma_2\widehat{U}\} = ord_p\gamma_1\widehat{V}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_1$.

$$ord_p\hat{X} = ord_p\gamma_1\widehat{V} - ord_p\gamma_1 = ord_p\widehat{V} = \frac{1}{3}ord_p\frac{G_0}{4a}.$$

We will obtain the same result if $\min\{ord_p\gamma_1\widehat{V}, ord_p\gamma_2\widehat{U}\} = ord_p\gamma_1\widehat{V}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_2$.
Suppose next $\min\{ord_p\gamma_1\widehat{V}, ord_p\gamma_2\widehat{U}\} = ord_p\gamma_2\widehat{U}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_2$.

$$ord_p\hat{X} = ord_p\gamma_2\widehat{U} - ord_p\gamma_2 = ord_p\widehat{U} = \frac{1}{3}ord_p\frac{F_0}{4a}.$$

We will obtain the same result if $\min\{ord_p\gamma_1\widehat{V}, ord_p\gamma_2\widehat{U}\} = ord_p\gamma_2\widehat{U}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_1$.
Considering all the cases above, we have

$$ord_p\hat{X} \geq \frac{1}{3}ord_p\frac{H_0}{4a}$$ where H_0 is either G_0 or F_0, from which

$$ord_p\hat{X} \geq \frac{1}{3}\{ord_p[f_x(x_0, y_0) + \lambda f_y(x_0, y_0)] - ord_p a\}.$$

Now, $ord_p[f_x(x_0, y_0) + \lambda f_y(x_0, y_0)] \geq \min\{ord_p f_x(x_0, y_0), ord_p\lambda f_y(x_0, y_0)\}$.
Suppose $\min\{ord_p f_x(x_0, y_0), ord_p\lambda f_y(x_0, y_0)\} = ord_p f_x(x_0, y_0)$, then

$$ord_p\hat{X} \geq \frac{1}{3}(ord_p f_x(x_0, y_0) - ord_p a) \geq \frac{1}{3}(\alpha - \delta).$$

Next, suppose that $\min\{ord_p f_x(x_0, y_0), ord_p\lambda f_y(x_0, y_0)\} = ord_p\lambda f_y(x_0, y_0)$, then $ord_p\hat{X} \geq \frac{1}{3}(ord_p\lambda f_y(x_0, y_0) - ord_p a)$ where $ord_p\lambda = \frac{1}{2}ord_p\frac{a}{b}$ from Lemma 3
Thus,

$$ord_p\hat{X} \geq \frac{1}{3}\left(ord_p f_y(x_0, y_0) + \frac{1}{2}ord_p\frac{a}{b} - ord_p a\right) = \frac{1}{3}\left(ord_p f_y(x_0, y_0) - \frac{1}{2}ord_p b - \frac{1}{2}ord_p a\right).$$

From which it follow that,

$$ord_p\hat{X} \geq \frac{1}{3}\left(\alpha - \frac{1}{2}\delta - \frac{1}{2}\delta\right)$$
$$\geq \frac{1}{3}(\alpha - \delta).$$

Next we consider equation (14). We have the following four cases.
First we suppose $\min\{ord_p\hat{V}, ord_p\hat{U}\} = ord_p\hat{U}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_1$.

$$ord_p\hat{Y} = ord_p\hat{U} - ord_p\gamma_1$$
$$= \frac{1}{3}ord_p\frac{F_0}{4a} - ord_p\frac{b\lambda_1}{6a}$$
$$= \frac{1}{3}ord_pF_0 + \frac{2}{3}ord_pa - ord_pb\lambda_1 .$$

Next, suppose $\min\{ord_p\hat{V}, ord_p\hat{U}\} = ord_p\hat{U}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_2$. Then we obtain

$$ord_p\hat{Y} = ord_p\hat{U} - ord_p\gamma_2$$
$$ord_p\hat{Y} = \frac{1}{3}ord_p\frac{F_0}{4a} - ord_p\frac{b\lambda_2}{6a}$$
$$= \frac{1}{3}ord_pF_0 + \frac{2}{3}ord_pa - ord_pb\lambda_2 .$$

Suppose $\min\{ord_p\hat{V}, ord_p\hat{U}\} = ord_p\hat{V}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_1$.

$$ord_p\hat{Y} = ord_p\hat{V} - ord_p\gamma_1$$
$$= \frac{1}{3}ord_p\frac{G_0}{4a} - ord_p\frac{b\lambda_1}{6a}$$
$$= \frac{1}{3}ord_pG_0 + \frac{2}{3}ord_pa - ord_pb\lambda_1.$$

Suppose $\min\{ord_p\hat{V}, ord_p\hat{U}\} = ord_p\hat{V}$ and $\min\{ord_p\gamma_1, ord_p\gamma_2\} = ord_p\gamma_2$.

$$ord_p\hat{Y} = ord_p\hat{V} - ord_p\gamma_2$$
$$= \frac{1}{3}ord_p\frac{G_0}{4a} - ord_p\frac{b\lambda_2}{6a}$$
$$= \frac{1}{3}ord_pG_0 + \frac{2}{3}ord_pa - ord_pb\lambda_2 .$$

Considering all the cases above, we have

$ord_p\hat{Y} \geq \frac{1}{3}ord_pH_0 + \frac{2}{3}ord_pa - ord_pb\lambda$ where H_0 is either G_0 or F_0 and λ is either λ_1 or λ_2. That is

$$ord_p\hat{Y} \geq \frac{1}{3}ord_p[f_x(x_0,y_0) + \lambda f_y(x_0,y_0)] + \frac{2}{3}ord_pa - ord_pb - ord_p\lambda.$$

Now $ord_p[f_x(x_0,y_0) + \lambda f_y(x_0,y_0)] \geq \min\{ord_pf_x(x_0,y_0), ord_p\lambda f_y(x_0,y_0)\}$.
Suppose $\min\{ord_pf_x(x_0,y_0), ord_p\lambda f_y(x_0,y_0)\} = ord_p\lambda f_y(x_0,y_0)$, then

$$ord_p\hat{Y} \geq \frac{1}{3}ord_p\lambda f_y(x_0,y_0) + \frac{2}{3}ord_pa - ord_pb - ord_p\lambda$$
$$= \frac{1}{3}ord_pf_y(x_0,y_0) + \frac{2}{3}ord_pa - ord_pb - \frac{1}{3}ord_p\frac{a}{b} \text{ from Lemma 3}$$
$$> \frac{1}{3}\left(ord_pf_y(x_0,y_0) - 2ord_pb\right).$$

Thus,

$$ord_p\hat{Y} > \frac{1}{3}(\alpha - 2\delta).$$

Suppose next $\min\{ord_p f_x(x_0,y_0), ord_p\lambda f_y(x_0,y_0)\} = ord_p f_x(x_0,y_0)$, then

$$ord_p\hat{Y} \geq \frac{1}{3}ord_p f_x(x_0,y_0) + \frac{2}{3}ord_p a - ord_p b - ord_p\lambda$$
$$= \frac{1}{3}ord_p f_x(x_0,y_0) + \frac{2}{3}ord_p a - \left(ord_p a - 2ord_p\lambda\right) - ord_p\lambda$$

since $ord_p b = ord_p a - 2ord_p\lambda$ from Lemma 3.

$$ord_p\hat{Y} \;= \frac{1}{3}ord_p f_x(x_0,y_0) + ord_p\lambda - \frac{1}{3}ord_p a\ .$$

Suppose $ord_p\lambda \geq 0$, then

$$ord_p\hat{Y} \geq \frac{1}{3}\left(ord_p f_x(x_0,y_0) - ord_p a\right)$$
$$\geq \frac{1}{3}(\alpha - \delta).$$

Suppose $ord_p\lambda < 0$, then

$$ord_p\hat{Y} \geq \frac{1}{3}ord_p f_x(x_0,y_0) + ord_p\lambda - \frac{1}{3}ord_p a$$
$$= \frac{1}{3}ord_p f_x(x_0,y_0) + \frac{1}{2}ord_p\frac{a}{b} - \frac{1}{3}ord_p a \text{ from Lemma 3}$$
$$> \frac{1}{3}\left(ord_p f_x(x_0,y_0) - \frac{3}{2}ord_p b\right).$$

Thus,

$$ord_p\hat{Y} > \frac{1}{3}\left(\alpha - \frac{3}{2}\delta\right) > \frac{1}{3}(\alpha - 2\delta).$$

Hence, $ord_p\hat{X} \geq \frac{1}{3}(\alpha-\delta)$ and $ord_p\hat{Y} \geq \frac{1}{3}(\alpha-\delta)$ or $ord_p\hat{Y} > \frac{1}{3}(\alpha-2\delta)$.

Let $\xi = \hat{X} + x_0$ and $\eta = \hat{Y} + y_0$, then $\hat{X} = \xi - x_0$ and $\hat{Y} = \eta - y_0$.

Thus, we have

$ord_p(\xi - x_0) \geq \frac{1}{3}(\alpha-\delta)$, $ord_p(\eta - y_0) \geq \frac{1}{3}(\alpha-\delta)$ or $ord_p(\eta - y_0) > \frac{1}{3}(\alpha-2\delta)$.

By back substitution in (7), (8) and (4), we have $f_x(\xi,\eta) = 0$ and $f_y(\xi,\eta) = 0$.

□

ESTIMATION OF $N(g,h,p^\alpha)$

Consider quartic polynomial $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + +rx + sy + t$. The cardinality of set of solution to congruence equations of partial derivative polynomials associated with $f(x,y)$ will be obtained in this section. The cardinality associated with $f\,(x,y)$ under the condition $ord_p ac^2 > ord_p b^3$ will be given in Theorem 4. We first have the following theorem given by Loxton and Vaughn (1985)

Theorem 3: Let p be a prime and $g(x,y), h(x,y)$ be a polynomials in $Q_p[x,y]$. Let $\alpha > 0$, (ξ_i,η_i), $i \geq 0$ be common zeros of g and h, $\gamma_i(\alpha) = inf_{x\in H_i(\alpha)}\{ord_p(x-\xi_i), ord_p(y-\eta_i)\}$ where $H(\alpha) = \cup_i H_i(\alpha)$. If $\alpha > \gamma_i(\alpha)$, then $N(g,h;p^\alpha) \leq \sum_i p^{2(\alpha-\gamma_i(\alpha))}$.

Theorem 4 : Let $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + +rx + sy + t$ be a polynomial in $Z_p[x,y]$ with $p > 3$. Let $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b, ord_p c, ord_p d\}$. Suppose $ord_p ac^2 > ord_p b^3$ and $2b^3 + 27ac^2 = 72abd$. Then

$$N(f_x,f_y;p^\alpha) \leq \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 9p^{\frac{4}{3}(\alpha+\delta)} & \text{if } \alpha > \delta. \end{cases}$$

Proof:

Suppose first that $\alpha \le \delta$. It is trivial that

$$N(f_x, f_y; p^\alpha) \le p^{2\alpha}.$$

Suppose next , $\alpha > \delta$. From Theorem 3

$$N(g, h; p^\alpha) \le \sum_i p^{2(\alpha - \gamma_i(\alpha))}$$

where

$$\gamma_i(\alpha) = \inf_{(x,y)\in H(\alpha)} \{ord_p(x - \xi_i), ord_p(x - \eta_i)\}.$$

We let $g = f_x$, $h = f_y$. Since $ord_p ac^2 > ord_p b^3$ and $2b^3 + 27ac^2 = 72abd$. By Theorem 1,

$$\gamma_i(\alpha) > \tfrac{1}{3}(\alpha - 2\delta).$$

By Bezout's Theorem, the number of common zeros doesn't exceed the product of the degree of f_x and f_y. Thus,

$$N(f_x, f_y; p^\alpha) \le 9p^{2\left(\alpha - \frac{1}{3}(\alpha - 2\delta)\right)} = 9p^{2\left(\frac{2}{3}\alpha + \frac{2}{3}\delta\right)} \text{ if } \alpha > \delta.$$

That is,

$$N(f_x, f_y; p^\alpha) \le 9p^{\frac{4}{3}(\alpha+\delta)}.$$

Therefore, we have

$$N(f_x, f_y; p^\alpha) \le \begin{cases} p^{2\alpha} & \text{if } \alpha \le \delta \\ 9p^{\frac{4}{3}(\alpha+\delta)} & \text{if } \alpha > \delta. \end{cases}$$

□

ESTIMATION OF EXPONENTIAL SUMS

Now, the estimation of the cardinality is used in order to estimate the exponential sums of the associated polynomials. Mohd Atan (1986) gives the following two theorems for α is an even and odd numbers respectively.

Theorem 5: Let p be a prime and $f(x,y)$ be a polynomial in $Z_p[x,y]$. For $\alpha > 1$, let $S(f; p^\alpha) = \sum_{x,y \bmod p} e^{\frac{2\pi i f(x)}{p^\alpha}}$, then $|S(f; p^\alpha)| \le p^{2(\alpha-\theta)} N_{f_x f_y}(p^\theta)$, where $\theta = \left[\frac{\alpha}{2}\right]$.

Theorem 6: Let p be a prime and $f(x,y)$ be a polynomial in $Z_p[x,y]$. Let $\alpha = 2\beta + 1$ with $\beta \ge 1$. Then, $|S(f; p^\alpha)| \le p^{\alpha+1} N_{f_x f_y}(p^\beta)$.

The estimation of multiple exponential sums associated with quartic polynomial in the form of $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + +rx + sy + t$ under the condition $ord_p ac^2 > ord_p b^3$ as in the theorem below.

Theorem 7: Let p be an odd prime and $\alpha > 1$. Let $f(x,y) = ax^4 + bx^2y^2 + cxy^3 + dy^4 + rx + sy + t$ be a polynomial in $Z_p[x,y]$ with $p > 3$. Let $\delta = \max\{ord_p a, ord_p b, ord_p c, ord_p d\}$, $ord_p ac^2 > ord_p b^3$ and $2b^3 + 27ac^2 = 72abd$. Then

$$|S(f; p^\alpha)| \le \begin{cases} p^{2\alpha} & \text{if } \alpha \le \delta \\ 9p^{\frac{1}{3}(5\alpha+4\delta+1)} & \text{if } \alpha > \delta. \end{cases}$$

Proof:

Suppose first that $\alpha \le \delta$. It is obvious that

$$|S(f;p^{\alpha})| \le p^{2\alpha}.$$

Suppose next $\alpha > \delta$. Since $ord_p ac^2 > ord_p b^3$ and $2b^3 + 27ac^2 = 72abd$, then by Theorem 4,

$$N(f_x, f_y; p^{\alpha}) \le 9p^{\frac{4}{3}(\theta+\delta)} \tag{15}$$

where $\theta = \left[\frac{\alpha}{2}\right]$ and $\delta = \max\{ord_p a, ord_p b, ord_p c, ord_p d\}$.

If $\alpha = 2\theta$, then by (15) and Theorem 5, we obtain

$$\begin{aligned} |S(f;p^{\alpha})| &\le p^{2(\alpha-\theta)} \cdot 9p^{\frac{4}{3}(\theta+\delta)} \\ &= 9p^{\frac{5}{3}\alpha+\frac{4}{3}\delta} \end{aligned}$$

That is, $|S(f;p^{\alpha})| \le 9p^{\frac{1}{3}(5\alpha+4\delta)}$.

Suppose α is odd, that is $\alpha = 2\beta + 1$ where $\beta > 0$. By Theorem 5,

$$|S(f;p^{\alpha})| \le p^{\alpha+1} N(f_x, f_y; p^{\beta}).$$

By Theorem 4, we have

$$N(f_x, f_y; p^{\beta}) \le 9p^{\frac{4}{3}(\beta+\delta)}.$$

Thus,

$$|S(f;p^{\alpha})| \le 9p^{\alpha+1+\frac{4}{3}\beta+\frac{4}{3}\delta}.$$

Let $2\beta = \alpha - 1$, then

$$|S(f;p^{\alpha})| \le 9p^{\frac{5}{3}\alpha+\frac{4}{3}\delta+\frac{1}{3}}.$$

That is,

$$|S(f;p^{\alpha})| \le 9p^{\frac{1}{3}(5\alpha+4\delta+1)} \quad \text{if } \alpha \text{ is odd.}$$

Therefore,

$$|S(f;p^{\alpha})| \le \begin{cases} p^{2\alpha} & \text{if } \alpha \le \delta \\ 9p^{\frac{1}{3}(5\alpha+4\delta+1)} & \text{if } \alpha > \delta \end{cases}$$

for all $\alpha > 0$.

□

CONCLUSION

In this paper, the p-adic sizes of partial derivative polynomials associated with quartic polynomial in the form of $f(x,y) = ax^4 + bx^3y + cxy^3 + dy^4 + rx + sy + t$ is considered. Then, by using these results, the estimation of cardinality of the set $(f_x, f_y; p^{\alpha})$ was found. After that, the result of the cardinality is then used to estimate the exponential sums of the quartic polynomial $f(x,y)$.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude and appreciation to the Putra grant UPM/700-2/1/GBP/2017/9597900 that has enabled us to carry out this research.

REFERENCES

Chan, K.L. and Mohd. Atan, K.A., On the Estimate to Solutions of Congruence Equations Associated with a Quartic Form. *J. Phys. Sci.* 8: (1997) 21-34.

Loxton J.H and Vaughan R.C., The Estimate of Complete Exponential Sums, *Canad. Math. Bull.,* 28 (4), (1985), 440-454.

Mohd Atan K.A. and Abdullah I., On the Estimate to Solutions of Congruence Equation Associated with Cubic Form, *Pertanika,*1 (2), (1993), 249-260.

Mohd Atan, K. A, Newton Polyhedral Method of Determining p-adic Orders of Common Zeros to Two Polynomials in $Q_p[x, y]$, *Pertanika*, 9 (3), (1986), 375-380.

Sapar, S. and Mohd Atan, K.A, Estimates for the Cardinality of the Set of Solution to Congruence Equations (Malay)*, Jurnal Teknologi,* 36**,** (2002), 13-40.

Sapar, S. and Mohd Atan, K.A., A Method of Estimating the p-adic sizes of Common Zeros of Partial Derivative Polynomials Associated with a Quintic Form*, International Journal of Number Theory,* 5 (03), (2009), 541-554.

Sapar S. H., K.A. Mohd Atan and Aminuddin, S.S, On the Cardinality of the Set of Solutions to Congruence Equation Associated with Cubic Form, *JP Journal of Algebra, Number Theory and Application*, 33 (1), (2014), 1-14.

Yap H. K., Mohd Atan K.A and Sapar S.H, Estimation of p-adic sizes of Common Zeros of Partial Derivative Polynomials Associated with a Cubic Form*, Sains Malaysiana*, 40 (8), (2011), 921-926.