Malaysian Journal of Mathematical Sciences 14(1): 115–138 (2020)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Exponential Sums for Eighth Degree Polynomial

Low, C. W. [1], Sapar, S. H. * [1,2], and Johari, M. A. M.[1,2]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

E-mail: sitihas@upm.edu.my
* *Corresponding author*

Received: 29 October 2018
Accepted: 30 September 2019

ABSTRACT

Let $p > 7$ be a prime, the exponential sums of any polynomial $f(x, y)$ is given by $S(f; p^\alpha) = \sum_{x,y \ mod \ p} e^{\frac{2\pi i f(x,y)}{p^\alpha}}$, where the sum is taken over a complete set of residue modulo p. Firstly, Newton Polyhedron technique was used to determine the estimation for the p-adic sizes of common zeros of the partial derivative polynomials f_x, f_y which derive from $f(x, y)$. We continue by estimating the cardinality $N(g, h; p^\alpha)$ as well as the exponential sums of polynomial $f(x, y)$. Throught out this paper, we consider the polynomial of eighth degree with two variables in the form $f(x, y) = ax^8 + bx^7y + cx^6y^2 + dx^5y^3 + ex^4y^4 + kx^3y^5 + mx^2y^6 + nxy^7 + uy^8 + rx + sy + t$.

Keywords: p-adic sizes, Newton Polyhedron, Indicator diagram, Cardinality, Exponential sums.

1. Introduction

In this section, we begin by giving some definition that will be used through out this paper. we define $\mathbb{Z}_p$ as the field of p-adic integer. Ω_p defines as the completion of algebraic closure of the field of rational p-adic numbers Q_p. ord_p x is the highest power of p which divides x, or the number of times that x can be divided by p.

Loxton and Smith (1982) obtained that the cardinality $N(f, p^\alpha)$ can be determined by the p-adic sizes of common zeros of partial derivative polynomials associated with f in the neighbourhood of points in the product space Ω_p^n, $n > 0$.

Loxton and Vaughan (1985) studied the exponential sums $S(f;q) = \sum_{x \ mod \ q} exp\ (2\pi i f/q)$ of a nonlinear polynomial f in $\mathbb{Z}[x]$. They used the number of common zeros of the partial derivative polynomials of f with respect to x modulo q to estimate the value of exponential sums.

Mohd Atan and Loxton (1986) estimate the p-adic sizes of polynomials in $\Omega_p[x, y]$ by using p-adic Newton polyhedral method which is an analogue of Newton polygon defined by Koblitz (1977). They obtained an estimation of cardinality for certain lower-degree polynomials $f(x, y)$ over $\mathbb{Z}_p$.

Many researchers also used Newton polyhedron technique for lower degree two-variable polynomials in Mohd Atan, Chan and Mohd Atan (1997), Heng and Mohd Atan (1999) as well as Sapar and Mohd Atan (2002). However, for the higher degree polynomials, the results are less complete.

Then, Sapar and Mohd Atan (2009) found that the p-adic sizes of common zeros of partial derivative polynomials associated with a quintic form for prime $p > 5$ by using Newton polyhedral technique.

Yap et al. (2011) proved that with the help of Newton polyhedron technique, the p-adic sizes of common zeros of partial derivative polynomials associated with a cubic form can be found explicitly. The overlapping segment of the indicator diagrams associated with the polynomials are the p-adic sizes of common zeros.

Sapar et al. (2013) studied the estimation of p-adic sizes of common zeros of degree nine polynomial. Aminudin et al. (2014) continued the finding of Yap et al. (2011) on a complete cubic form polynomial. They found that the result is not the same as in Yap et al. (2011). Thus, the different form of cubic

polynomials will get the different p-adic sizes. In addition, Sapar et al. (2014) investigated the estimation of p-adic sizes of a eighth degree polynomial.

Zulkapli et al. (2015) investigated the p-adic sizes of factorials. The result is in explicit forms and the method of obtaining them offers an alternative way in finding $ord_p n!$. Other than that, they found the p-adic sizes of ${}^nC_r$ where $n = p^\alpha$ and $r = p^\theta$ for $\alpha > \theta > 0$.

Lasaraiya et al. (2016a) studied the cardinality of the polynomial of degree eleven in the form $f(x, y) = ax^{11} + bx^{10}y + cx^9y^2 + sx + ty + k$. They found out that the cardinality is given by

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 100p^{2(9\delta+\frac{3}{2}\epsilon_0+8\epsilon_1+10q)} & \text{if } \alpha > \delta \end{cases}$$

where $p > 11$ is a prime, $\alpha > 1$, $\epsilon_0, \epsilon_1, q \geq 0$ and $\delta = \max\{ord_p\, a, ord_p\, b, ord_p\, c\}$.

Last but not least, Lasaraiya et al. (2016b) investigated the cardiality of twelfth degree polynimial in the form $f(x, y) = ax^{12}+bx^{11}y+cx^{10}y^2+sx+ty+k$. The results are as follow:

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 121p^{2(11\delta+\frac{3}{2}\epsilon_0+9\epsilon_1+11q)} & \text{if } \alpha > \delta \end{cases}$$

where $p > 11$ is a prime, $\alpha > 1$, $\epsilon_0, \epsilon_1, q \geq 0$ and $\delta = \max\{ord_p\, a, ord_p\, b, ord_p\, c\}$.

In this paper, we apply the Newton polyhedron technique to determine the p-adic sizes of the partial derivative polynomials of $f(x, y)$ in $\mathbb{Z}_p[x, y]$ of a degree eight. Then, we obtain the estimation of cardinality and the exponential sums of the polynomial $f(x, y) = ax^8 + bx^7y + cx^6y^2 + dx^5y^3 + ex^4y^4 + kx^3y^5 + mx^2y^6 + nxy^7 + uy^8 + rx + sy + t$.

2. p-Adic Size of Common Zero of Polynomial

In this section, we find the p-adic sizes of common zeros of partial derivative polynomial $f(x, y)$ at the neighbourhood (x_0, y_0) as stated. Sapar and Mohd Atan (2002) proved that every point of intersection of the indicator diagrams, there exist common zeros of both polynomials in $\mathbb{Z}_p[x, y]$ whose p-adic orders correspond to point (μ_1, μ_2) as in the following theorem:

Theorem 1
Let p be a prime. Suppose f and g are polynomials in $\mathbb{Z}_p[x, y]$. Let (μ_1, μ_2)

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 $ord_p\ \xi = \mu_1,\ ord_p\ \eta = \mu_2$.

The following lemmas are needed to prove our main result as shown in Theorem 2.

Lemma 1
For $p > 7$ where p is a prime. Let $a, b, c, d, e, k, m, n, u$ in $\mathbb{Z}_p$ and λ_1, λ_2 are the zeros of $z(\lambda) = (560cu - 8em)\lambda^2 + (70cn + 1960bu - 10dm - 4ek)\,\lambda + (245bn - 5dk)$. If

$$\alpha_1 = \frac{7b + 2\lambda_1 c}{7(8a + \lambda_1 b)} \text{ and } \alpha_2 = \frac{7b + 2\lambda_2 c}{7(8a + \lambda_2 b)},$$

then

$$\begin{aligned} ord_p(\alpha_1 - \alpha_2) = \frac{1}{2}\ ord_p[&(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em) \\ &(245bn - 5dk)] - ord_p(560cu - 8em) + ord_p(16ac - 7b^2) \\ &- ord_p(8a + \lambda_1 b) - ord_p(8a + \lambda_2 b). \end{aligned}$$

Proof.

$$\alpha_1 - \alpha_2 = \frac{7b + 2\lambda_1 c}{7(8a + \lambda_1 b)} - \frac{7b + 2\lambda_2 c}{7(8a + \lambda_2 b)} = \frac{(\lambda_1 - \lambda_2)(16ac - 7b^2)}{7(8a + \lambda_1 b)(8a + \lambda_2 b)}.$$

Take ord_p on both sides, we have

$$ord_p(\alpha_1 - \alpha_2) = ord_p(\lambda_1 - \lambda_2) + ord_p(16ac - 7b^2) - ord_p(8a + \lambda_1 b) - ord_p(8a + \lambda_2 b)$$

where

$$\lambda_1 - \lambda_2 = \frac{\sqrt{(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em)(245bn - 5dk)}}{(560cu - 8em)}.$$

Therefore,

$$\begin{aligned} ord_p(\alpha_1 - \alpha_2) = \frac{1}{2}\ ord_p[&(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em) \\ &(245bn - 5dk)] - ord_p(560cu - 8em) + ord_p(16ac - 7b^2) \\ &- ord_p(8a + \lambda_1 b) - ord_p(8a + \lambda_2 b). \end{aligned}$$

□

In the following lemma, α_1 and α_2 are denoted as follow:

$$\alpha_1 = \frac{7b + 2\lambda_1 c}{7(8a + \lambda_1 b)} \text{ and } \alpha_2 = \frac{7b + 2\lambda_2 c}{7(8a + \lambda_2 b)}.$$

Lemma 2
Suppose $(X + x_0, Y + y_0)$ in Ω_p^2, $U = x + \alpha_1 y$ and $V = x + \alpha_2 y$. Let $p > 7$ where p is a prime, $a, b, c, d, e, k, m, n, u, r, s$ in $\mathbb{Z}_p$, $ord_p\ r, ord_p\ s \geq \alpha > \delta$ and $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c, ord_p\ d,\ ord_p\ e, ord_p\ k, ord_p\ m, ord_p\ n, ord_p\ u\}$. If $ord_p\ U = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_1 s}{8a+\lambda_1 b}\right)$ and $ord_p\ V = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right)$ with the condition $ord_p(70cn + 1960bu - 10dm - 4ek)^2 \neq ord_p\ 4(560cu - 8em)(245bn - 5dk)$, then

$$ord_p(X + x_0) \geq \frac{1}{7}(\alpha - 40\delta),$$

$$ord_p(Y + y_0) \geq \frac{1}{7}(\alpha - 26\delta).$$

Proof. Let $x = X + x_0$ and $y = Y + y_0$. Then, $U = (X + x_0) + \alpha_1(Y + y_0)$ and $V = (X + x_0) + \alpha_2(Y + y_0)$, we have

$$(X + x_0) = \frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2} \text{ and } (Y + y_0) = \frac{U - V}{\alpha_1 - \alpha_2}.$$

Then, $ord_p(X + x_0)$ and $ord_p(Y + y_0)$ will be as follow:

$$ord_p(X + x_0) = ord_p(\alpha_1 V - \alpha_2 U) - ord_p(\alpha_1 - \alpha_2), \tag{1}$$

$$ord_p(Y + y_0) = ord_p(U - V) - ord_p(\alpha_1 - \alpha_2). \tag{2}$$

From (2),

$$ord_p(Y + y_0) \geq \min\{ord_p\ U, ord_p\ V\} - ord_p\ (\alpha_1 - \alpha_2)\,.$$

By Lemma 1, we have

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p[(70cn + 1960bu - 10dm - 4ek)^2 \\ & - 4(560cu - 8em)(245bn - 5dk)] + ord_p(560cu - 8em) \\ & - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) + ord_p(8a + \lambda_2 b). \end{aligned} \tag{3}$$

Since $ord_p(70cn + 1960bu - 10dm - 4ek)^2 \neq ord_p\ 4(560cu - 8em)(245bn - 5dk)$, we consider two cases.

Case (i):
$ord_p(70cn + 1960bu - 10dm - 4ek)^2 > ord_p\ 4(560cu - 8em)(245bn - 5dk)$,

Case (ii):
$ord_p(70cn + 1960bu - 10dm - 4ek)^2 < ord_p\ 4(560cu - 8em)(245bn - 5dk)$.

For **Case (i)**, equation (3) becomes

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p[4(560cu - 8em)(245bn - 5dk)] \\ & + ord_p(560cu - 8em) - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) \\ & + ord_p(8a + \lambda_2 b). \end{aligned} \tag{4}$$

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p(245bn - 5dk) + \frac{1}{2}\ ord_p(560cu - 8em) \\ & - ord_p(16ac - 7b^2) + ord_p[(8a + \lambda_1 b)(8a + \lambda_2 b)]. \end{aligned}$$

We continue with another two cases which are $\min\{ord_p\ U, ord_p\ V\} = ord_p\ U$ and $\min\{ord_p\ U, ord_p\ V\} = ord_p\ V$. If $\min\{ord_p\ U, ord_p\ V\} = ord_p\ U$, we have

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \frac{1}{7}\ ord_p(r + \lambda_1 s) - \frac{1}{2}\ ord_p(245bn - 5dk) + \frac{1}{2}\ ord_p(560cu - 8em) \\ & - ord_p(16ac - 7b^2) + \frac{6}{7}\ ord_p[(8a + \lambda_1 b)(8a + \lambda_2 b)]. \end{aligned}$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$\begin{aligned} ord_p(Y + y_0) \geq & \frac{1}{7}\ ord_p(r + \lambda_1 s) - \frac{1}{2}\ ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) \\ & - \frac{5}{14}\ ord_p(560cu - 8em). \end{aligned}$$

If $\min\{ord_p\ U, ord_p\ V\} = ord_p\ V$, we have

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \frac{1}{7}\ ord_p(r + \lambda_2 s) - \frac{1}{2}\ ord_p(245bn - 5dk) + \frac{1}{2}\ ord_p(560cu - 8em) \\ & - ord_p(16ac - 7b^2) + \frac{6}{7}\ ord_p[(8a + \lambda_1 b)(8a + \lambda_2 b)]. \end{aligned}$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$ord_p(Y + y_0) \geq \frac{1}{7}\ ord_p(r + \lambda_2 s) - \frac{1}{2}\ ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) - \frac{5}{14}\ ord_p(560cu - 8em).$$

So, we can conclude that for **Case (i)**, we obtain the following result.

$$ord_p(Y + y_0) \geq \frac{1}{7}\min\{ord_p\ r, ord_p\ \lambda_i s\} - \frac{1}{2}\min\{ord_p\ bn, ord_p\ dk\} - \min\{ord_p\ ac, ord_p\ b^2\} - \frac{5}{14}\min\{ord_p\ cu, ord_p\ em\}$$

where $i = 1, 2$.

By hypothesis, we have

$$ord_p(Y + y_0) \geq \frac{1}{7}(\alpha - 26\delta). \tag{5}$$

For **Case (ii)**, equation (3) becomes

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p[(70cn + 1960bu - 10dm - 4ek)^2] \\ & + ord_p(560cu - 8em) - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) \\ & + ord_p(8a + \lambda_2 b). \end{aligned}$$

But since
$ord_p(70cn + 1960bu - 10dm - 4ek)^2 < ord_p\ 4(560cu - 8em)(245bn - 5dk)$, then

$$\begin{aligned} ord_p(Y + y_0) \geq\ & \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p[4(560cu - 8em)(245bn - 5dk)] \\ & + ord_p(560cu - 8em) - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) \\ & + ord_p(8a + \lambda_2 b). \end{aligned}$$

It is exactly same as equation (4), thus the result will be same as equation (5).

From equation (1), we have

$$ord_p(X + x_0) \geq \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - ord_p(\alpha_1 - \alpha_2).$$

By Lemma 1, we obtain

$$\begin{aligned} ord_p(X+x_0) \geq\ & \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p[(70cn+1960bu-10dm-4ek)^2 \\ & - 4(560cu-8em)(245bn-5dk)] + ord_p(560cu-8em) \\ & - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b). \end{aligned} \tag{6}$$

Since $ord_p(70cn+1960bu-10dm-4ek)^2 \neq ord_p\ 4(560cu-8em)(245bn-5dk)$, we consider two cases.

Case (iii):
$ord_p(70cn+1960bu-10dm-4ek)^2 > ord_p\ 4(560cu-8em)(245bn-5dk)$,

Case (iv):
$ord_p(70cn+1960bu-10dm-4ek)^2 < ord_p\ 4(560cu-8em)(245bn-5dk)$.

For **Case (iii)**, equation (6) becomes

$$\begin{aligned} ord_p(X+x_0) \geq\ & \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p[4(560cu-8em)(245bn-5dk)] \\ & + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) \\ & + ord_p(8a+\lambda_2 b). \end{aligned} \tag{7}$$

$$\begin{aligned} ord_p(X+x_0) \geq\ & \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p(245bn-5dk) + \frac{1}{2}\ ord_p(560cu-8em) \\ & - ord_p(16ac-7b^2) + ord_p[(8a+\lambda_1 b)(8a+\lambda_2 b)]. \end{aligned}$$

We continue with another two cases which are:

$\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_1 V$ and $\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_2 U$.

If $\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_1 V$, we have

$$\begin{aligned} ord_p(X+x_0) \geq\ & \frac{1}{7}\ ord_p(r+\lambda_2 s) + ord_p(7b+2\lambda_1 c) - \frac{1}{2}\ ord_p(245bn-5dk) \\ & + \frac{1}{2}\ ord_p(560cu-8em) - ord_p(16ac-7b^2) + \frac{6}{7}\ ord_p(8a+\lambda_2 b). \end{aligned}$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p(r+\lambda_2 s) - \frac{1}{2}\ ord_p(245bn-5dk) - ord_p(16ac-7b^2) - \frac{19}{14}\ ord_p(560cu-8em).$$

If $\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_2 U$, we have

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p(r+\lambda_1 s) + ord_p(7b+2\lambda_2 c) - \frac{1}{2}\ ord_p(245bn-5dk) + \frac{1}{2}\ ord_p(560cu-8em) - ord_p(16ac-7b^2) + \frac{6}{7}\ ord_p(8a+\lambda_1 b).$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p(r+\lambda_1 s) - \frac{1}{2}\ ord_p(245bn-5dk) - ord_p(16ac-7b^2) - \frac{19}{14}\ ord_p(560cu-8em).$$

We can conclude that for **Case (iii)**, the result will be as follow:

$$ord_p(X+x_0) \geq \frac{1}{7}\min\{ord_p\ r, ord_p\ \lambda_i s\} - \frac{1}{2}\min\{ord_p\ bn, ord_p\ dk\} - \min\{ord_p\ ac, ord_p\ b^2\} - \frac{19}{14}\min\{ord_p\ cu, ord_p\ em\}$$

where $i = 1, 2$.

By hypothesis, we get

$$ord_p(X+x_0) \geq \frac{1}{7}(\alpha - 40\delta).$$

For **Case (iv)**, equation (6) becomes

$$ord_p(X+x_0) \geq \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p(70cn+1960bu-10dm-4ek)^2 + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

But since
$ord_p(70cn+1960bu-10dm-4ek)^2 < ord_p\ 4(560cu-8em)(245bn-5dk)$, then

$$ord_p(X+x_0) \geq \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p[4(560cu-8em)(245bn-5dk)] + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

It is exactly same as (7). As a result,

$$ord_p(X+x_0) \geq \frac{1}{7}(\alpha - 40\delta).$$

□

Next, we continue with another lemma for condition,
$ord_p(70cn+1960bu-10dm-4ek)^2 = ord_p\ 4(560cu-8em)(245bn-5dk)$.

Lemma 3
Suppose $(X+x_0, Y+y_0)$ is in Ω_p^2, $U = x+\alpha_1 y$ and $V = x+\alpha_2 y$. Let $p > 7$ where p is a prime, $a, b, c, d, e, k, m, n, u, r, s$ in $\mathbb{Z}_p$, $ord_p\ r, ord_p\ s \geq \alpha > \delta$ and $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c, ord_p\ d,\ ord_p\ e, ord_p\ k, ord_p\ m, ord_p\ n, ord_p\ u\}$. If $ord_p\ U = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_1 s}{8a+\lambda_1 b}\right)$ and $ord_p\ V = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right)$ with the condition $ord_p(70cn+1960bu-10dm-4ek)^2 = ord_p\ 4(560cu-8em)(245bn-5dk)$, then

$$ord_p(X+x_0) \geq \frac{1}{7}(\alpha - 40\delta) - \frac{1}{2}\omega_0$$

$$ord_p(Y+y_0) \geq \frac{1}{7}(\alpha - 26\delta) - \frac{1}{2}\omega_0$$

for some $\omega_0 \geq 0$.

Proof. From Lemma 2, we have

$$ord_p(Y+y_0) \geq \min\{ord_p\ U, ord_p\ V\} - \frac{1}{2}\ ord_p[(70cn+1960bu-10dm-4ek)^2 - 4(560cu-8em)(245bn-5dk)] + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

If $\min\{ord_p\ U, ord_p\ V\} = ord_p\ U$ and we substitute the expression of $ord_p\ U$, we will obtain

$$\begin{aligned} ord_p(Y + y_0) \geq \frac{1}{7}\ ord_p\left(\frac{r + \lambda_1 s}{8a + \lambda_1 b}\right) - \frac{1}{2}\ ord_p[(70cn + 1960bu - 10dm - 4ek)^2 \\ - 4(560cu - 8em)(245bn - 5dk)] + ord_p(560cu - 8em) \\ - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) + ord_p(8a + \lambda_2 b). \end{aligned}$$

Now, let
$ord_p(70cn + 1960bu - 10dm - 4ek)^2 = ord_p\ 4(560cu - 8em)(245bn - 5dk) = \gamma$,
we have

$$(70cn + 1960bu - 10dm - 4ek)^2 = Ap^{\gamma}$$

and

$$4(560cu - 8em)(245bn - 5dk) = Bp^{\gamma}$$

where $ord_p\ A = ord_p\ B = 0$.

Then,

$$\begin{aligned} &ord_p[(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em)(245bn - 5dk)] \\ &= ord_p(Ap^{\gamma} - Bp^{\gamma}) \\ &= ord_p\ p^{\gamma} + ord_p(A - B) \\ &= \gamma + \omega_0 \end{aligned}$$

where $\omega_0 = ord_p(A - B) \geq 0$. Now,

$$\begin{aligned} ord_p(Y + y_0) \geq \frac{1}{7}\ ord_p\left(\frac{r + \lambda_1 s}{8a + \lambda_1 b}\right) - \frac{1}{2}(\gamma + \omega_0) + ord_p(560cu - 8em) \\ - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) + ord_p(8a + \lambda_2 b). \end{aligned}$$

We choose $\gamma = ord_p\ 4(560cu - 8em)(245bn - 5dk)$, then

$$\begin{aligned} ord_p(Y + y_0) \geq \frac{1}{7}\ ord_p(r + \lambda_1 s) + \frac{1}{2}\ ord_p(560cu - 8em) - \frac{1}{2}\ ord_p(245bn - 5dk) \\ - ord_p(16ac - 7b^2) + \frac{6}{7}\ ord_p(8a + \lambda_1 b)(8a + \lambda_2 b) - \frac{1}{2}\omega_0. \end{aligned}$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have,

$$ord_p(Y + y_0) \geq \frac{1}{7}\, ord_p(r + \lambda_1 s) - \frac{1}{2}\, ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) - \frac{5}{14}\, ord_p(560cu - 8em) - \frac{1}{2}\omega_0.$$

If $\min\{ord_p\ U, ord_p\ V\} = ord_p\ V$ and we substitute the expression of $ord_p\ V$, we will obtain

$$ord_p(Y + y_0) \geq \frac{1}{7}\, ord_p\left(\frac{r + \lambda_2 s}{8a + \lambda_2 b}\right) - \frac{1}{2}\, ord_p[(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em)(245bn - 5dk)] + ord_p(560cu - 8em) - ord_p(16ac - 7b^2) + ord_p(8a + \lambda_1 b) + ord_p(8a + \lambda_2 b).$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$ord_p(Y + y_0) \geq \frac{1}{7}\, ord_p(r + \lambda_2 s) - \frac{1}{2}\, ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) - \frac{5}{14}\, ord_p(560cu - 8em) - \frac{1}{2}\omega_0.$$

Therefore,

$$ord_p(Y + y_0) \geq \frac{1}{7}\, ord_p(r + \lambda_i s) - \frac{1}{2}\, ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) - \frac{5}{14}\, ord_p(560cu - 8em) - \frac{1}{2}\omega_0$$

where $i = 1, 2$.

By hypothesis, we obtain

$$ord_p(Y + y_0) \geq \frac{1}{7}(\alpha - 26\delta) - \frac{1}{2}\omega_0$$

for some $\omega_0 \geq 0$.

Also, from Lemma 2, we have

$$ord_p(X+x_0) \geq \min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} - \frac{1}{2}\ ord_p[(70cn+1960bu-10dm-4ek)^2 - 4(560cu-8em)(245bn-5dk)] + ord_p(560cu-8em) - ord_p(16c-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

If $\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_1 V$. We substitute the expressions of $ord_p\ V$ and $ord_p\ \alpha_1$ expression of α_1, then

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right) + ord_p\left(\frac{7b+2\lambda_1 c}{7(8a+\lambda_1 b)}\right) - \frac{1}{2}\ ord_p[(70cn+1960bu-10dm-4ek)^2 - 4(560cu-8em)(245bn-5dk)] + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

We consider
$ord_p(70cn+1960bu-10dm-4ek)^2 = ord_p\ 4(560cu-8em)(245bn-5dk) = \gamma$, then

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right) + ord_p\left(\frac{7b+2\lambda_1 c}{7(8a+\lambda_1 b)}\right) - \frac{1}{2}(\gamma+\omega_0) + ord_p(560cu-8em) - ord_p(16ac-7b^2) + ord_p(8a+\lambda_1 b) + ord_p(8a+\lambda_2 b).$$

We choose $\gamma = ord_p\ 4(560cu-8em)(245bn-5dk)$, then

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p(r+\lambda_2 s) + ord_p(7b+2\lambda_1 c) + \frac{1}{2}\ ord_p(560cu-8em) + \frac{6}{7}\ ord_p(8a+\lambda_2 b) - \frac{1}{2}\ ord_p(245bn-5dk) - ord_p(16ac-7b^2) - \frac{1}{2}\omega_0.$$

By substituting the values of λ_1, λ_2 and simplifying the expression above, we have

$$ord_p(X+x_0) \geq \frac{1}{7}\ ord_p(r+\lambda_2 s) - \frac{1}{2}\ ord_p(245bn-5dk) - ord_p(16ac-7b^2) - \frac{19}{14}\ ord_p(560cu-8em) - \frac{1}{2}\omega_0.$$

For the case $\min\{ord_p\ \alpha_1 V, ord_p\ \alpha_2 U\} = ord_p\ \alpha_2 U$ and substitute the expressions of $ord_p\ U$ and $ord_p\ \alpha_2$, we have

$$\begin{aligned} ord_p(X + x_0) \geq \frac{1}{7}\ ord_p\left(\frac{r + \lambda_1 s}{8a + \lambda_1 b}\right) + ord_p\left(\frac{7b + 2\lambda_2 c}{7(8a + \lambda_2 b)}\right) \\ - \frac{1}{2}\ ord_p[(70cn + 1960bu - 10dm - 4ek)^2 - 4(560cu - 8em) \\ (245bn - 5dk)] + ord_p(560cu - 8em) - ord_p(16ac - 7b^2) \\ + ord_p(8a + \lambda_1 b) + ord_p(8a + \lambda_2 b). \end{aligned}$$

We continue in the similar manner and substitute the values of λ_1 and λ_2, at the end we have

$$\begin{aligned} ord_p(X + x_0) \geq \frac{1}{7}\ ord_p(r + \lambda_1 s) - \frac{1}{2}\ ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) \\ - \frac{19}{14}\ ord_p(560cu - 8em) - \frac{1}{2}\omega_0. \end{aligned}$$

Therefore,

$$\begin{aligned} ord_p(X + x_0) \geq \frac{1}{7}\ ord_p(r + \lambda_i s) - \frac{1}{2}\ ord_p(245bn - 5dk) - ord_p(16ac - 7b^2) \\ - \frac{19}{14}\ ord_p(560cu - 8em) - \frac{1}{2}\omega_0 \end{aligned}$$

where $i = 1, 2$. By hypothesis, we obtain

$$ord_p(X + x_0) \geq \frac{1}{7}(\alpha - 40\delta) - \frac{1}{2}\omega_0$$

for some $\omega_0 \geq 0$ as asserted.

□

Theorem 2
Let $f(x, y) = ax^8 + bx^7y + cx^6y^2 + dx^5y^3 + ex^4y^4 + kx^3y^5 + mx^2y^6 + nxy^7 + uy^8 + rx + sy + t$ be a polynomial in $\mathbb{Z}_p[x, y]$ with $p > 7$ is a prime. Let $\alpha > 0$, $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c, ord_p\ d, ord_p\ e, ord_p\ k, ord_p\ m, ord_p\ n, ord_p\ u\}$.

If $ord_p\ f_x(x - x_0, y - y_0), ord_p\ f_y(x - x_0, y - y_0) \geq \alpha > \delta$, then there exists (ζ, η) such that $f_x(\zeta, \eta) = 0$, $f_y(\zeta, \eta) = 0$ and

$ord_p(70cn + 1960bu - 10dm - 4ek)^2 \neq ord_p\ 4(560cu - 8em)(245bn - 5dk)$	$ord_p(70cn + 1960bu - 10dm - 4ek)^2 = ord_p\ 4(560cu - 8em)(245bn - 5dk)$
$ord_p(\zeta - x_0) \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_1$	$ord_p(\zeta - x_0) \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_3 - \frac{1}{2}\omega_0$
$ord_p(\eta - y_0) \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_2$	$ord_p(\eta - y_0) \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_4 - \frac{1}{2}\omega_0$.

for some $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \omega_0 \geq 0$.

Proof. Let

$$g = f_x(x,y) = 8ax^7+7bx^6y+6cx^5y^2+5dx^4y^3+4ex^3y^4+3kx^2y^5+2mxy^6+ny^7+r,$$
$$h = f_y(x,y) = bx^7+2cx^6y+3dx^5y^2+4ex^4y^3+5kx^3y^4+6mx^2y^5+7nxy^6+8uy^7+s,$$

and

$$x = X + x_0,$$
$$y = Y + y_0.$$

Then

$$\begin{aligned}\frac{g+\lambda h}{8a+\lambda b} = {} & (X+x_0)^7 + \left(\frac{7b+2\lambda c}{8a+\lambda b}\right)(X+x_0)^6(Y+y_0) + \left(\frac{6c+3\lambda d}{8a+\lambda b}\right) \\ & (X+x_0)^5(Y+y_0)^2 + \left(\frac{5d+4\lambda e}{8a+\lambda b}\right)(X+x_0)^4(Y+y_0)^3 + \\ & \left(\frac{4e+5\lambda k}{8a+\lambda b}\right)(X+x_0)^3(Y+y_0)^4 + \left(\frac{3k+6\lambda m}{8a+\lambda b}\right)(X+x_0)^2 \\ & (Y+y_0)^5 + \left(\frac{2m+7\lambda n}{8a+\lambda b}\right)(X+x_0)(Y+y_0)^6 + \left(\frac{n+8\lambda u}{8a+\lambda b}\right) \\ & (Y+y_0)^7 + \left(\frac{r+\lambda s}{8a+\lambda b}\right)\end{aligned}$$

By completing the seventh degree, we have

$$\frac{g+\lambda h}{8a+\lambda b} = \left[(X+x_0) + \frac{1}{7}\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)(Y+y_0)\right]^7 + \left(\frac{r+\lambda s}{8a+\lambda b}\right)$$

with

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^2 - \frac{7}{3}\left(\frac{6c+3\lambda d}{8a+\lambda b}\right) = 0 \tag{8}$$

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^3 - \frac{49}{5}\left(\frac{5d+4\lambda e}{8a+\lambda b}\right) = 0 \tag{9}$$

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^4 - \frac{343}{5}\left(\frac{4e+5\lambda k}{8a+\lambda b}\right) = 0 \tag{10}$$

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^5 - \frac{2401}{3}\left(\frac{3k+6\lambda m}{8a+\lambda b}\right) = 0 \tag{11}$$

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^6 - 7^5\left(\frac{2m+7\lambda n}{8a+\lambda b}\right) = 0 \tag{12}$$

$$\left(\frac{7b+2\lambda c}{8a+\lambda b}\right)^7 - 7^7\left(\frac{n+8\lambda u}{8a+\lambda b}\right) = 0. \tag{13}$$

By solving the equation (8) to equation (13) simultaneously, we obtain

$$(560cu - 8em)\lambda^2 + (70cn + 1960bu - 10dm - 4ek)\lambda + (245bn - 5dk) = 0.$$

Thus,

$$\lambda = \frac{-L \pm \sqrt{L^2 - 4KM}}{2K}$$

where

$$K = 560cu - 8em,$$
$$L = 70cn + 1960bu - 10dm - 4ek,$$
$$M = 245bn - 5dk.$$

Let

$$U = (X + x_0) + \frac{1}{7}\left(\frac{7b + 2\lambda_1 c}{8a + \lambda_1 b}\right)(Y + y_0) \tag{14}$$

$$V = (X + x_0) + \frac{1}{7}\left(\frac{7b + 2\lambda_2 c}{8a + \lambda_2 b}\right)(Y + y_0), \tag{15}$$

we have

$$g + \lambda_1 h = (8a + \lambda_1 b)\, U^7 + r + \lambda_1 s \tag{16}$$

$$g + \lambda_2 h = (8a + \lambda_2 b)\, V^7 + r + \lambda_2 s. \tag{17}$$

We let

$$F(U, V) = (g + \lambda_1 h) = (8a + \lambda_1 b)\, U^7 + r + \lambda_1 s \tag{18}$$

$$G(U, V) = (g + \lambda_2 h) = (8a + \lambda_2 b)\, V^7 + r + \lambda_2 s. \tag{19}$$

Based on equation (18), we obtain two points in the Newton diagram which are

$$A = (7, 0, ord_p(8a + \lambda_1 b))$$
$$B = (0, 0, ord_p(r + \lambda_1 s))$$

and the vector

$$\vec{AB} = \left(-7, 0, ord_p\left(\frac{r + \lambda_1 s}{8a + \lambda_1 b}\right)\right).$$

Next, we multiply the vector $\vec{AB}$ with its normal $(U, V, 1)$ to get the $ord_p\, U$ as shown as below:

$$\vec{AB} \cdot (U, V, 1) = \quad 0$$
$$\left(-7, 0, ord_p\left(\frac{r + \lambda_1 s}{8a + \lambda_1 b}\right)\right) \cdot (U, V, 1) = \quad 0.$$

Therefore, we have

$$ord_p\ U = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_1 s}{8a+\lambda_1 b}\right).$$

From equation (19), we use the same argument as above and we obtain the vector

$$\vec{CD} = \left(0, -7, ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right)\right).$$

Same as previous, we multiply the vector $\vec{CD}$ with its normal $(U, V, 1)$ to get the $ord_p\ V$:

$$\begin{aligned}\vec{CD}\cdot(U,V,1) &= 0\\ \left(0,-7,ord_p\left(\frac{r+\lambda_2 s}{8+\lambda_2 b}\right)\right)\cdot(U,V,1) &= 0.\end{aligned}$$

Therefore, we have

$$ord_p\ V = \frac{1}{7}\ ord_p\left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right).$$

The combination of the indicator diagrams associated with the Newton polyhedron of (16) and (17) as shown in Figure 1. By Theorem 1, there exists a point $(\hat{U}, \hat{V})$ such that $F(\hat{U}, \hat{V}) = 0$ and $G(\hat{U}, \hat{V}) = 0$. Let (μ_1, μ_2) be the point of intersection in the indicator diagrams such that $\mu_1 = ord_p\ \hat{U} = \frac{1}{7}\ ord_p\ \left(\frac{r+\lambda_1 s}{8a+\lambda_1 b}\right)$ and $\mu_2 = ord_p\ \hat{V} = \frac{1}{7}\ ord_p\ \left(\frac{r+\lambda_2 s}{8a+\lambda_2 b}\right)$.

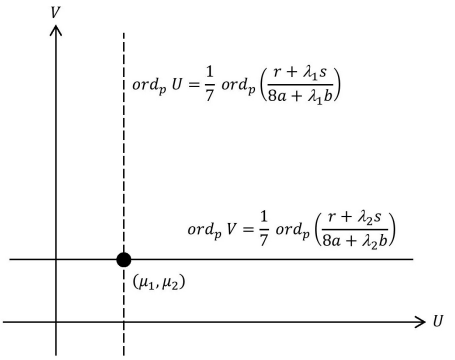

Figure 1: The indicator diagrams for the polynomials of $F(U,V) = (g+\lambda_1 h) = (8a+\lambda_1 b)\,U^7 + r + \lambda_1 s$ (broken line) and $G(U,V) = (g+\lambda_2 h) = (8a+\lambda_2 b)\,V^7 + r + \lambda_2 s$ (solid line) with $p = 3$.

Let $U = \hat{U}$ and $V = \hat{V}$. From (14) and (15), there exists $(\hat{X} + \hat{x}_0)$ and $(\hat{Y} + \hat{y}_0)$ in such a way that:

$$(\hat{X} + \hat{x}_0) = \frac{\alpha_1 \hat{V} - \alpha_2 \hat{U}}{\alpha_1 - \alpha_2}$$

$$(\hat{Y} + \hat{y}_0) = \frac{\hat{U} - \hat{V}}{\alpha_1 - \alpha_2}$$

where $\alpha_1 = \frac{7b+2\lambda_1 c}{7(8a+\lambda_1 b)}$, $\alpha_2 = \frac{7b+2\lambda_2 c}{7(8a+\lambda_2 b)}$ and λ_1, λ_2 are the zeros of $z(\lambda) = (560cu - 8em)\lambda^2 + (70cn + 1960bu - 10dm - 4ek)\lambda + (245bn - 5dk)$ for $\lambda_1 \neq \lambda_2$, $\alpha_1 \neq \alpha_2$.

Next, we want to find $ord_p\ \hat{X}$ and $ord_p\ \hat{Y}$. From Lemma 2, we have,

$$ord_p(\hat{X} + \hat{x}_0) \geq \frac{1}{7}(\alpha - 40\delta)$$

and

$$ord_p(\hat{Y} + \hat{y}_0) \geq \frac{1}{7}(\alpha - 26\delta).$$

By the property $ord_p(A \pm B) \geq \min\{ord_p A, ord_p B\}$, we have,

$$ord_p(\hat{X} + \hat{x}_0) = ord_p\ \hat{X} + \epsilon_1$$

$$ord_p(\hat{Y} + \hat{y}_0) = ord_p\ \hat{Y} + \epsilon_2$$

for some $\epsilon_1, \epsilon_2 \geq 0$.

This will result as

$$ord_p\ \hat{X} \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_1,$$

$$ord_p\ \hat{Y} \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_2.$$

We let $\zeta = \hat{X} + \hat{x}_0$ and $\eta = \hat{Y} + \hat{y}_0$, then

$$ord_p(\zeta - \hat{x}_0) \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_1$$

and

$$ord_p(\eta - \hat{y}_0) \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_2.$$

By back substitution, we have $g(\zeta, \eta) = f_x(\zeta, \eta) = 0$ and $h(\zeta, \eta) = f_y(\zeta, \eta) = 0$.

From Lemma 3, we have

$$ord_p(\hat{X} + \hat{x}_0) \geq \frac{1}{7}(\alpha - 40\delta) - \frac{1}{2}\omega_0$$

and

$$ord_p(\hat{Y} + \hat{y}_0) \geq \frac{1}{7}(\alpha - 26\delta) - \frac{1}{2}\omega_0.$$

By the property $ord_p(A \pm B) \geq \min\{ord_p A, ord_p B\}$, we have,

$$ord_p(\hat{X} + \hat{x}_0) = ord_p\ \hat{X} + \epsilon_3$$

$$ord_p(\hat{Y} + \hat{y}_0) = ord_p\ \hat{Y} + \epsilon_4$$

for some $\epsilon_3, \epsilon_4 \geq 0$.

This will result as

$$ord_p\ \hat{X} \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_3 - \frac{1}{2}\omega_0,$$

$$ord_p\ \hat{Y} \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_4 - \frac{1}{2}\omega_0.$$

We let $\zeta = \hat{X} + \hat{x}_0$ and $\eta = \hat{Y} + \hat{y}_0$, then

$$ord_p(\zeta - \hat{x}_0) \geq \frac{1}{7}(\alpha - 40\delta) - \epsilon_3 - \frac{1}{2}\omega_0$$

and

$$ord_p(\eta - \hat{y}_0) \geq \frac{1}{7}(\alpha - 26\delta) - \epsilon_4 - \frac{1}{2}\omega_0.$$

By back substitution, we have $g(\zeta, \eta) = f_x(\zeta, \eta) = 0$ and $h(\zeta, \eta) = f_y(\zeta, \eta) = 0$. □

3. Estimation of Cardinality

In this section, we obtain the cardinality $N(g, h; p^\alpha)$ of the sixth degree polynomial. From Loxton and Smith (1982), we can obtain the $N(g, h; p^\alpha)$ from the p-adic size of $ord_p(x - \zeta_i)$ and $ord_p(y - \eta_i)$ by the following theorem.

Theorem 3
Let p be a prime and $g(x,y)$ and $h(x,y)$ are polynomials in $Q_p[x,y]$. Let $\alpha > 0$, $(\zeta_i, \eta_i), i \geq 0$ be common zeros of g and h, and

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

where $H(\alpha) = \cup_i H_i(\alpha)$. If $\alpha > \gamma_i(\alpha)$, then $N(g,h;p^\alpha) \leq \sum_i p^{2(\alpha-\gamma_i(\alpha))}$.

Next, we can prove the following theorem.

Theorem 4
Let $f(x,y) = ax^8 + bx^7y + cx^6y^2 + dx^5y^3 + ex^4y^4 + kx^3y^5 + mx^2y^6 + nxy^7 + uy^8 + rx + sy + t$ be a polynomial in $\mathbb{Z}_p[x,y]$ with $p > 7$ is a prime. Let $\alpha > 0$, $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c, ord_p\ d, ord_p\ e, ord_p\ k, ord_p\ m, ord_p\ n, ord_p\ u\}$, then

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 49p^{80\delta+14q} & \text{if } \alpha > \delta \end{cases}$$

where $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$.

Proof. Suppose $\alpha \leq \delta$, it is very obvious that $N(f_x, f_y; p^\alpha) \leq p^{2\alpha}$ since $\gamma_i(\alpha) = 0$.

Next, suppose $\alpha > \delta$. From Theorem 3, we have

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

for $\gamma_i(\alpha) = \inf_{x \in H(\alpha)}\{ord_p(x-\zeta_i), ord_p(y-\eta_i)\}$ where $H(\alpha) = \cup_i H_i(\alpha)$. $\gamma_i(\alpha)$ is the minimum value of $ord_p(x-\zeta_i)$ and $ord_p(y-\eta_i)$ in order to get the upper bound of $N(f_x, f_y; p^\alpha)$. From Theorem 2, we have

$$ord_p(\zeta - x_0) \geq \frac{1}{7}(\alpha - 40\delta) - q$$

where $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$. Thus,

$$\alpha - 7\gamma_i(\alpha) \leq 40\delta + 7q.$$

From Bezout's Theorem, the product of the degrees of f_x and f_y is the maximum number of the common zeros. Therefore,

$$N(f_x, f_y; p^\alpha) \leq 49p^{80\delta+14q}$$

for $\alpha > \delta$ and $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$. □

4. Estimation of Exponential Sums

In this section, we obtain the estimation of of exponential sums. The exponential sums is given by

$$S(f;p^{\alpha}) = \sum_{x,y \ mod \ p} e^{\frac{2\pi i f(x,y)}{p^{\alpha}}}$$

where $f(x,y)$ is a polynomial in $\mathbb{Z}_p[x,y]$. The sum is taken over a complete set of residues x modulo positive integer p^{α} with $\alpha \geq 1$.

In order to obtain the exponential sums of a sixth degree polynomial, we need the theorems from Mohd Atan (1984) as stated below.

Theorem 5
Let p be a prime and $f(x,y)$ be a polynomial in $\mathbb{Z}_p[x,y]$. For $\alpha > 1$, let

$$S(f;p^{\alpha}) = \sum_{x,y \ mod \ p} e^{\frac{2\pi i f(x,y)}{p^{\alpha}}},$$

then

$$|S(f;p^{\alpha})| \leq p^{2(\alpha-\theta)} N_{f_x f_y}(p^{\theta})$$

where $\theta = \frac{\alpha}{2}$.

The above theorem correct when α is even. But if α is odd, then we will use the following theorem to approach.

Theorem 6
Let p be a prime and $f(x,y)$ be a polynomial in $\mathbb{Z}_p[x,y]$. Let $\alpha = 2\beta + 1$ where $\beta \geq 1$ and

$$S(f;p^{\alpha}) = \sum_{x,y \ mod \ p} e^{\frac{2\pi i f(x,y)}{p^{\alpha}}},$$

then

$$|S(f;p^{\alpha})| \leq p^{2\beta+2} N_{f_x f_y}(p^{\beta}).$$

By using the above two theorems, we have the following result.

Theorem 7
Let $f(x,y) = ax^8+bx^7y+cx^6y^2+dx^5y^3+ex^4y^4+kx^3y^5+mx^2y^6+nxy^7+uy^8+rx+sy+t$ be a polynomial in $\mathbb{Z}_p[x,y]$. Suppose $p > 7$ is a prime and $\alpha > 1$. Let $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c, ord_p\ d, ord_p\ e, ord_p\ k, ord_p\ m, ord_p\ n, ord_p\ u\}$, then

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 49p^{\alpha+1+80\delta+14q}\}$$

where $q = \max\{\epsilon_3, \epsilon_4\}$.

Proof. From Theorem 4, we have

$$N(f_x, f_y; p^\alpha) \leq \min\{p^{2\alpha}, 49p^{80\delta+14q}\}$$

where $\theta = \frac{\alpha}{2}$ and $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$.

Suppose α is even. If $\alpha > 1$ and $\alpha = 2\theta$. From Theorem 5, we have,

$$\begin{aligned} |S(f;p^\alpha)| &\leq p^{2(\alpha-\theta)} \min\{p^{2\theta}, 49p^{42\delta+7\omega_0+14q}\} \\ &= \min\{p^{2\alpha}, 49p^{\alpha+80\delta+14q}\}. \end{aligned}$$

Suppose α is odd. If $\alpha > 1$ and $\alpha = 2\beta + 1$. From Theorem 6, we have,

$$\begin{aligned} |S(f;p^\alpha)| &\leq p^{2\beta+2} \min\{p^{2\beta}, 49p^{80\delta+14q}\} \\ &= \min\{p^{2\alpha}, 49p^{\alpha+1+80\delta+14q}\}. \end{aligned}$$

□

5. Conclusion

In this paper, we use a complete dominant terms of sixth degree polynomial with two variables. We found that the exponential sums of polynomial $f(x,y)$ is given by

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 49p^{\alpha+1+80\delta+14q}\}$$

where p, q, α, δ are stated previously.

References

Aminudin, S. S., Sapar, S. H., and Mohd Atan, K. A. (2014). A method of estimating the p-adic sizes of common zeros of partial derivative polynomials associated with a complete cubic form. In *International Conference on Mathematical Sciences and Statistics 2013*, pages 205–212. Springer.

Chan, K. L. and Mohd Atan, K. A. (1997). On the estimate to solutions of congruence equations associated with a quartic form. *J. Phys. Sci*, 8:21–34.

Heng, S. H. and Mohd Atan, K. A. (1999). An estimation of exponential sums associated with a cubic form. *Physical Sci*, 10:1–21.

Koblitz, N. (1977). P-adic numbers. In *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, pages 1–20. Springer.

Lasaraiya, S., Sapar, S. H., and Johari, M. A. M. (2016a). On the cardinality of the set of solutions to congruence equation associated with polynomial of degree eleven. In *AIP Conference Proceedings*, volume 1750, page 050015. AIP Publishing.

Lasaraiya, S., Sapar, S. H., and Johari, M. A. M. (2016b). On the cardinality of twelfth degree polynomial. In *AIP Conference Proceedings*, volume 1739, page 020008. AIP Publishing.

Loxton, J. H. and Smith, R. A. (1982). Estimates for multiple exponential sums. *Journal of the Australian Mathematical Society*, 33(1):125–134.

Loxton, J. H. and Vaughan, R. C. (1985). The estimation of complete exponential sums. *Can. Math. Bull.*, 28(4):440–454.

Mohd Atan, K. A. Newton polyhedral method of determining p-adic orders of zeros common to two polynomials in q[x, y]. *Pertanika*, 9(3):375–380.

Mohd Atan, K. A. (1984). *Newton Polyhedral and Estimates for Exponential Sums*. PhD thesis, University of New South Wales, Kensington, Australia.

Mohd Atan, K. A. and Loxton, J. H. (1986). Newton polyhedra and solutions of congruences. *Diophantine analysis (Kensington, 1985)*, pages 67–82.

Sapar, S. H., Aminudin, S. S., and Mohd Atan, K. A. (2014). A method of estimating the p-adic sizes polynomials. *International Journal of Pure Mathematics*, 1:22–29.

Sapar, S. H. and Mohd Atan, K. A. (2002). Estimate for the cardinality of the set of solution to congruence equations. *Journal of Technology*, 36:13–40.

Sapar, S. H. and Mohd Atan, K. A. (2009). 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):541–554.

Sapar, S. H., Mohd Atan, K. A., and Aminuddin, S. S. (2013). An estimating the p-adic sizes of common zeros of partial derivative polynomials. *New Trends in Mathematical Sciences*, 1(1):38–48.

Yap, H. K., Mohd Atan, K. A., and Sapar, S. H. (2011). Estimation of p-adic sizes of common zeros of partial derivatives associated with a cubic form. *Sains Malaysiana*, 40(8):921–926.

Zulkapli, R., Mohd Atan, K. A., and Sapar, S. H. (2015). A method for determining p-adic orders of factorials. *Malaysian Journal of Mathematical Sciences*, 9(2):277–300.