CARDINALITY OF SETS ASSOCIATED TO CERTAIN DEGREE SEVEN POLYNOMIALS

Suriana Lasaraiya[1*], Siti Hasana Sapar[1,2] and Mohamat Aidil Mohamat Johari[2]

[1]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor.
[2]Mathematics Department, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor.
[*]Corresponding Author: Suriana13Lasaraiya@gmail.com

ABSTRACT Let $f = f(x, y)$ be a function of two variables. Let q be an integer and let $S(f; q) = \sum_{x \bmod q} e^{\frac{2\pi i f(x)}{q}}$, where the sum is taken over a complete set of residue modulo q. The value of $S(f; q)$ depends on the estimate of the cardinality $|V|$ of the following set $V = \{(x, y) mod\ q\ | f_x, f_y \equiv 0\ mod\ q\}$ where f_x and f_y are the partial derivative of f with respect to x and y. In this paper, we discuss the cardinality, $|V|$ of the set of solutions for congruence equations of some special binary forms. Firstly we need to obtain the p-adic sizes of common zeros of the partial derivative polynomials by using Newton polyhedron technique. The polynomial that we consider is in the form of $f(x, y) = ax^7 + bx^6y + cx^5y^2 + sx + ty + k$.

(**Keywords**:p-adic order, Newton Polyhedron, Indicator diagram, Cardinality)

INTRODUCTION

In our introduction, let p be a prime. We use the notations Z_p to denote the ring of p-adic integers, Q_p is the field of p-adic, $\bar{Q}_p$ is the closure of Q_p and Ω_p is to denote the algebraically closed and a complete extensions of the field $\bar{Q}_p$ respectively. For a rational number of x, we denote the p-adic size of x as $ord_p x$, we mean the highest power of p dividing x. A Newton Polyhedron associated with a polynomial $f(x, y) = \sum a_{ij} x^i y^j$ with the coefficient in Ω_p is the lower convex hull of the set of point $(i, j, ord_p a_{ij})$. It consists of faces and edges on and above which lie the point $(i, j, ord_p a_{ij})$. The Newton Polyhedron technique was extended and developed by [1] from the study of Koblitz (1977). After that, [2] obtain p-adic orders of common zeros of two polynomials in $Q_p[x, y]$ by examining the combination of indicator diagram associated with both polynomials obtained from the partial derivatives of$f(x, y)$.

Estimation of $N(f; p^\alpha)$has been made by [3].Then, [4] made the extension of estimation for such exponential sums with $f$is a cubic polynomials with coefficient in the ring Z. A method of estimating the p-adic order sizes has been done by [5] where the polynomials is in the form of quintic form. Estimation of p-adic size also done by [6] associated with a cubic degree polynomials. In the reference [7] the more involved case of degree nine polynomials has already been published. By using the same method, [8] has done the estimation on the cardinality of the set of solutions for the congruence equation associated with a cubic form.

In this paper, we will find the cardinality to certain degree seven polynomial. In order to determine the cardinality, we have to find the p-adic size of zeros of the polynomial byusing the Newton polyhedron technique and analyzing the combination of the indicator diagram.

RESULTS AND DISCUSSION

p-ADIC SIZES OF ZEROS OF A POLYNOMIAL

In this work, we discuss about the p-adic sizes of common zeros of partial derivative polynomials associated with a polynomial $f(x, y)$ of degree seven in $z_P[x, y]$ of the form$f(x, y) = ax^7 + bx^6y + cx^5y^2 + sx + ty + k$. Then, we will find the cardinality of the set of solutions to congruence equation of the polynomials. We need the following definitions and theorems developed by [1].

Definition 1 : (Newton Diagram)

Let $f(x, y) = \sum a_{ij} x^i y^j$be a polynomial of degree n in $\Omega_p[x, y]$. We map the terms $T_{ij} = a_{ij} x^i y^j$of $f(\mathrm{x,y})$to the point $P_{ij} = a_{ij} x^i y^j$in the three-dimensional Euclidean spaceR^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 $\Omega_p[x,y]$. We map the terms $T_{ij} = a_{ij}x^i y^j$of f(x,y) to the point $P_{ij} = a_{ij}x^i y^j$in the EuclideanspaceR^3. The Newton polyhedron of $f$is defined to be the lower convex hull of the set S of points P_{ij}, $O \leq i,j \leq$. 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 we take $ord_p a_{ij} = \infty$.

Definition 3 : (Indicator Diagram)

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 $\Omega_p[x,y]$. We map $(\mu_i, \lambda_i, 1)$ 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 $-\alpha/\beta$. We call the set of lines so obtained the Indicator Diagram associated with N_f.

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

From our investigation, we found that the p-adic size of the polynomials at any point with the conditions of $ord_p b^2 \neq ord_p ac$, that is for $ord_p b^2 > ord_p ac$ and $ord_p b^2 < ord_p ac$ as in the following theorem :

Theorem 2 Let $f(x,y) = ax^7 + bx^6y + cx^5y^2 + sx + ty + k$ be a polynomial in Q_p with $p > 7$ is a prime. Let $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ and (x_0, y_0) in Ω_p^2. If $ord_p b^2 \neq ord_p ac$, $ord_p f_x(x_0,y_0)$, $ord_p f_y(x_0,y_0) \geq \alpha > 7\delta$, then there exists (ξ,η) in Ω_p^2 such that $f_x(\xi,\eta) = 0$, $f_y(\xi,\eta) = 0$ and as follows :

$ord_p(\xi - x_0) \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_1$ and	$ord_p(\xi - x_0) \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_2$ and
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_4$or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$

for some $\varepsilon_0, \varepsilon_2, \varepsilon_4 \geq 0$ and $\varepsilon_1, \varepsilon_3 > 0$.

In order to prove Theorem 2, we need the results from the following lemmas that can be proved easily.

Lemma 2.1 Let $p > 7$ be a prime, a, b and c in Z_p and λ_1, λ_2 are the zeros of $k(\lambda) = \lambda^2c^2 + bc\lambda + 9b^2 - 35ac$. Let

$$\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b} \quad , \quad \alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b}$$

i) If $ord_p b^2 > ord_p ac$, then $ord_p\alpha_i = ord_p(\alpha_1 - \alpha_2) = \frac{1}{2}ord_p\frac{c}{a}$, $ord_p(\alpha_1 + \alpha_2) = ord_p\frac{b}{a}$ for $i = 1,2$ and ;

ii) If $ord_p b^2 < ord_p ac$, then $ord_p\alpha_i = ord_p(\alpha_1 - \alpha_2) = ord_p\frac{c}{b}$, $ord_p(\alpha_1 + \alpha_2) = ord_p\frac{c}{b}$ for $i = 1,2$

Throughout the following discussion, we used the notations

$$\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b} \quad , \quad \alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b} \qquad (1)$$

with λ_1, λ_2 are the zeros of $k(\lambda) = \lambda^2c^2 + bc\lambda + 9b^2 - 35ac$ and $\alpha_1 \neq \alpha_2$ since $\lambda_1 \neq \lambda_2$.

Lemma 2.2 Suppose (U,V) in Ω_p^2. Let $p > 7$ be a prime, a, b and c are coefficients of α_1 and α_2 as in Equation (1) in Z_p,
i) If $ord_p b^2 > ord_p ac$, then $ord_p(\alpha_1 V - \alpha_2 U) = ord_p\left[\sqrt{140ac - 35b^2}(U+V) + 5b(U-V)\right] - ord_p a$,

ii) If $ord_p b^2 < ord_p ac$, then $ord_p(\alpha_1 V - \alpha_2 U) = ord_p\left[\sqrt{140ac - 35b^2}(U + V) + 5b(U - V)\right] - ord_p \frac{b^2}{c}$.

Lemma 2.3 Suppose (x, y) in Ω_p^2 and $U = (X + x_0)^3 + \alpha_1(X + x_0)^2(Y + y_0)$, $V = (X + x_0)^3 + \alpha_2(X + x_0)^2(Y + y_0)$ where α_1 and α_2 as Equation (1). Let $p > 7$ be a prime, a, b and c are the coefficient of α_1 and α_2 in Z_p. Then,

$ord_p b^2 > ord_p ac$	$ord_p b^2 < ord_p ac$
$ord_p(X + x_0) \geq \frac{1}{3}W$	$ord_p(X + x_0) \geq \frac{1}{3}W$
$ord_p(Y + y_0) \geq \frac{1}{3}\left[W - \frac{1}{2}ord_p \frac{cb^4}{a^5}\right]$ or	$ord_p(Y + y_0) \geq \frac{1}{3}\left[W - \frac{1}{2}ord_p \frac{c^6}{b^6}\right]$ or
$ord_p(Y + y_0) \geq \frac{1}{3}\left[W - \frac{1}{2}ord_p \frac{cb^4}{a^5} - 2\varepsilon_0\right]$	$ord_p(Y + y_0) \geq \frac{1}{3}\left[W - \frac{1}{2}ord_p \frac{c^6}{b^6} - 2\varepsilon_0\right]$

in an exceptional case with $W = \min\{ord_p V, ord_p U\}$ and some $\varepsilon_0 \geq 0$ which can be specified explicitly.

Proof. From $U = (X + x_0)^3 + \alpha_1(X + x_0)^2(Y + y_0)$ and $V = (X + x_0)^3 + \alpha_2(X + x_0)^2(Y + y_0)$, we have

$$(X + x_0)^3 = \frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2}, \quad (Y + y_0) = \frac{U - V}{(\alpha_1 - \alpha_2)(X + x_0)^2}$$

Thus

$$ord_p(X + x_0) = \frac{1}{3}\left[ord_p(\alpha_1 V - \alpha_2 U) - ord_p(\alpha_1 - \alpha_2)\right] \qquad (2)$$

and

$$ord_p(Y + y_0) = ord_p(U - V) - ord_p(\alpha_1 - \alpha_2) - 2ord_p(X + x_0) \qquad (3)$$

From (2) and (3), we will consider two conditions with two cases for each conditions as follow:

CONDITION 1: $ord_p b^2 > ord_p ac$

In this condition, we will consider two cases. That is,

CASE I : $ord_p 5b(U - V) \neq ord_p \sqrt{140ac - 35b^2}(U + V)$

CASE II : $ord_p 5b(U - V) = ord_p \sqrt{140ac - 35b^2}(U + V)$

Now, we consider the Case I. Since $ord_p b^2 > ord_p ac$, $p > 7$ and by Lemmas (2.1) and (2.2), we have,

$$ord_p(X + x_0) = \frac{1}{3}\left[ord_p\left(\sqrt{140ac - 35b^2}(U + V) + 5b(U + V)\right) - \frac{1}{2}ord_p ac\right].$$

Suppose $\min\{ord_p 5b(U - V), ord_p \sqrt{140ac - 35b^2}(U + V)\} = ord_p \sqrt{140ac - 35b^2}(U + V)$. It follows that,

$$ord_p(X + x_0) = \frac{1}{3}ord_p \sqrt{140ac - 35b^2}(U + V) - \frac{1}{6}ord_p ac$$

Since $ord_p b^2 > ord_p ac$, we will have :

$$ord_p(X + x_0) = \frac{1}{3}ord_p(U + V) + \frac{1}{6}ord_p ac - \frac{1}{6}ord_p ac.$$

That is,

$$ord_p(X + x_0) = \frac{1}{3}ord_p(U + V) (4)$$

It follows that

$$ord_p(X + x_0) \geq \frac{1}{3}W$$

where $W = \min\{ord_p U, ord_p V\}$.

From definition of U and V,

$$ord_p(U + V) = ord_p[2(X + x_0)^3 + (\alpha_1 + \alpha_2)(X + x_0)^2(Y + y_0)]$$

From Equation (4)

$$ord_p(X + x_0)^3 = ord_p(U + V)$$

It can be shown that

$$ord_p(X + x_0) \leq ord_p(\alpha_1 + \alpha_2)(Y + y_0).$$

Hence, from equation (3) we will have

$$ord_p(Y + y_0) \geq \frac{1}{3}\left[ord_p(U - V) - \frac{1}{2}ord_p \frac{c}{a} - 2ord_p(\alpha_1 - \alpha_2)\right].$$

That is,

$$ord_p(Y + y_0) \geq \frac{1}{3}\left[ord_p(U - V) - \frac{1}{2}ord_p \frac{cb^4}{a^5}\right]. \qquad (5)$$

Therefore, in this case, we have

$$ord_p(X + x_0) \geq \frac{1}{3}W$$

and

$$ord_p(Y + y_0) \geq \frac{1}{3}\left[W - \frac{1}{2}ord_p \frac{cb^4}{a^5}\right].$$

Now, we have to consider Case II. That is, $ord_p 5b(U-V) = ord_p \sqrt{140ac-35b^2}(U+V)$.

Suppose $\min\{ord_p 5b(U-V), ord_p \sqrt{140ac-35b^2}(U+V)\} = ord_p \sqrt{140ac-35b^2}(U+V)$. It follows that,

$$ord_p(X+x_0) = \frac{1}{3} ord_p \sqrt{140ac-35b^2}(U+V) - \frac{1}{6} ord_p ac$$

Since $ord_p b^2 > ord_p ac$, we will have :

$$ord_p(X+x_0) = \frac{1}{3} ord_p(U+V) + \frac{1}{6} ord_p ac - \frac{1}{6} ord_p ac.$$

Therefore,

$$ord_p(X+x_0) = \frac{1}{3} ord_p(U+V)(6)$$

It follows that

$$ord_p(X+x_0) \geq \frac{1}{3} W$$

where $W = \min\{ord_p U, ord_p V\}$.

Let $ord_p \sqrt{140ac-35b^2}(U+V) = ord_p 5b(U-V) = \beta$.

Then, there exist k and l such that, $ord_p 5b(U-V) = ord_p p^\beta k$ and $ord_p \sqrt{140ac-35b^2}(U+V) = ord_p p^\beta l$ with $ord_p k = ord_p l = 0$.

From equation (3) and Lemma (2.1), we have

$$ord_p(Y+y_0) = ord_p(U-V) - \frac{1}{2} ord_p \frac{c}{a} - \frac{2}{3}\left[ord_p \sqrt{140ac-35b^2}(U+V) + 5b(U-V)\right] + \frac{1}{2} ord_p ac$$

$$ord_p(Y+y_0) = ord_p(U-V) - \frac{1}{2} ord_p \frac{c}{a} - \frac{2}{3} ord_p\left(p^\beta k + p^\beta l\right) + \frac{1}{2} ord_p ac$$

$$ord_p(Y+y_0) = \beta - ord_p b - \frac{1}{2} ord_p \frac{c}{a} - \frac{2}{3}\beta - \frac{2}{3} ord_p(k+l) + \frac{1}{3} ord_p ac$$

Thus,

$$ord_p(Y+y_0) = \frac{1}{3} ord_p(U-V) - \frac{2}{3}\varepsilon_0 - \frac{1}{6} ord_p \frac{cb^4}{a^5} \quad (7)$$

where $ord_p(k+l) = \varepsilon_0$.

In this case, we have

$$ord_p(X+x_0) \geq \frac{1}{3} W$$

and

$$ord_p(Y+y_0) = \frac{1}{3}\left[W - \frac{1}{2} ord_p \frac{cb^4}{a^5} - 2\varepsilon_0\right]$$

where $W = \min\{ord_p U, ord_p V\}$.

<u>CONDITION 2</u>: $ord_p b^2 < ord_p ac$

In this condition, we will consider two cases. That is,

CASE III :
$ord_p 5b(U-V) \neq ord_p \sqrt{140ac-35b^2}(U+V)$

CASE IV :
$ord_p 5b(U-V) = ord_p \sqrt{140ac-35b^2}(U+V)$

By using similar process as CONDITION 1, we will obtain :

For CASE III,

$$ord_p(X+x_0) \geq \frac{1}{3} W$$

and

$$ord_p(Y+y_0) = \frac{1}{3}\left[W - \frac{1}{2} ord_p \frac{c^6}{b^6}\right]$$

For CASE IV,

$$ord_p(X+x_0) \geq \frac{1}{3} W$$

and

$$ord_p(Y+y_0) = \frac{1}{3}\left[W - \frac{1}{2} ord_p \frac{c^6}{b^6} - 2\varepsilon_0\right]$$

With $W = \min\{ord_p U, ord_p V\}$ and $\varepsilon_0 \geq 0$ as asserted.

The following lemma gives explicit estimates of the p-adic sizes of $(X+x_0)$ and $(Y+y_0)$ in U, V where U and V as in Lemma (2.3). The proof utilizes the results obtained above.

Lemma 2.4 Suppose (x,y) in Ω_p^2 and $U = (X+x_0)^3 + \alpha_1(X+x_0)^2(Y+y_0)$, $V = (X+x_0)^3 + \alpha_2(X+x_0)^2(Y+y_0)$ where α_1 and α_2 as Equation (1). Let $p > 7$ be a prime, a, b, c, s and t in Z_p, $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ and $ord_p s, ord_p t \geq \alpha > \delta$. If $ord_p U = \frac{1}{2} ord_p \frac{s+\lambda_1 t}{7a+\lambda_1 b}$ and $ord_p V = \frac{1}{2} ord_p \frac{s+\lambda_2 t}{7a+\lambda_2 b}$, then the results will be as follows :

$ord_p b^2 > ord_p ac$	$ord_p b^2 < ord_p ac$
$ord_p(X+x_0) \geq \frac{1}{6}(\alpha-\delta)$	
Case I : $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-3\delta)$ or $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-4\delta)$	***Case II*** : $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-5\delta)$ or $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-6\delta)$
Case II : $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-3\delta)-\frac{2}{3}\varepsilon_0$ or $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-4\delta)-\frac{2}{3}\varepsilon_0$	***Case IV*** : $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-5\delta)-\frac{2}{3}\varepsilon_0$ or $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-4\delta)-\frac{2}{3}\varepsilon_0$

for some $\varepsilon_0 \geq 0$.

Proof. From Lemma (2.3), we have

$$ord_p(X+x_0) \geq \frac{1}{3}W$$

with $W = \min\{ord_p U, ord_p V\}$.

It follows that

$$ord_p(X+x_0) = \frac{1}{6} ord_p \frac{s+\lambda_i t}{7a+\lambda_i b}$$

for $i = 1,2$.

Then we have,

$$ord_p(X+x_0) = \frac{1}{6}\left[ord_p(s+\lambda_i t) - ord_p(7a+\lambda_i b)\right]$$

For both conditions, that is $ord_p b^2 > ord_p ac$ and $ord_p b^2 < ord_p ac$, we will have as in CASE A as follows :

Case (i) Suppose $\min\{ord_p s, ord_p \lambda_i t\} = ord_p s$ and $\min\{ord_p 7a, ord_p \lambda_i b\} = ord_p 7a$ or $\min\{ord_p 7a, ord_p \lambda_i b\} = ord_p \lambda_i b$, we have

$$ord_p(X+x_0) = \frac{1}{6}(\alpha-\delta).$$

Case (ii) Suppose $\min\{ord_p s, ord_p \lambda_i t\} = ord_p \lambda_i t$ and $\min\{ord_p 7a, ord_p \lambda_i b\} = ord_p 7a$ or $\min\{ord_p 7a, ord_p \lambda_i b\} = ord_p \lambda_i b$, we obtain

$$ord_p(X+x_0) = \frac{1}{6}(\alpha-\delta).$$

From Lemma (2.3), we have

$$ord_p(Y+y_0) \geq \frac{1}{6}\left[ord_p\left(\frac{s+\lambda_i t}{7a+\lambda_i b}\right) - ord_p \frac{cb^4}{a^5}\right]$$

for $i = 1,2$.

Then we have,

$$ord_p(Y+y_0) \geq \frac{1}{6}\left[ord_p(s+\lambda_i t) - ord_p(7a+\lambda_i b) - ord_p \frac{cb^4}{a^5}\right].$$

By using the same argument as in Case A, we have as shown below :

$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-3\delta)$	$ord_p(Y+y_0 \geq \frac{1}{6}(\alpha-5\delta)$
$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-4\delta)$	$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-6\delta)$
$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-3\delta)-\frac{2}{3}\varepsilon_0$	$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-5\delta)-\frac{2}{3}\varepsilon_0$
$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-4\delta)-\frac{2}{3}\varepsilon_0$	$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-6\delta)-\frac{2}{3}\varepsilon_0$

for some $\varepsilon_0 \geq 0$ as asserted.

The following theorem gives the p-adic sizes of common zeros of partial derivative polynomials associated with a polynomial $f(x,y)$ in $Z_p[x,y]$, in terms of the coefficient of its dominant terms.

Proof of Theorem 2.

Proof. Let $g = f_x$ and $h = f_y$ and λ be a constant. Then at $(X+x_0, Y+y_0)$, by completing the square, we have the following :

$$\frac{(g+\lambda h)(X+x_0,Y+y_0)}{(7a+\lambda b)} = [(X+x_0)^3 + \frac{(3b+\lambda c)}{(7a+\lambda b)}(X+x_0)^2(Y+y_0)]^2 + \frac{(s+\lambda t)}{(7a+\lambda b)}$$

Now let

$$U = (X+x_0)^3 + \frac{(3b+\lambda_1 c)}{(7a+\lambda_1 b)}(X+x_0)^2(Y+y_0) \quad (8)$$

$$V = (X+x_0)^3 + \frac{(3b+\lambda_2 c)}{(7a+\lambda_2 b)}(X+x_0)^2(Y+y_0) \quad (9)$$

Then, we have

$$F(U,V) = (g+\lambda_1 h)(X+x_0,Y+y_0) \quad (10)$$

$$G(U,V) = (g+\lambda_2 h)(X+x_0,Y+y_0) \quad (11)$$

Substitution of U and V into above equation, gives the following polynomials in (U,V),

$$F(U,V) = (7a + \lambda_1 b)U^2 + s + \lambda_1 t \quad (12)$$

$$G(U,V) = (7a + \lambda_2 b)U^2 + s + \lambda_2 t \quad (13)$$

By using Definition 1 and 2, we will get the combination of the indicator diagram associated with the Newton polyhedron of (10) and (11), as shown in Figure 1.

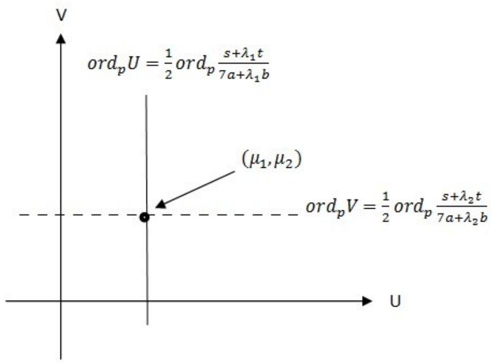

Figure 1. The indicator diagram of $F(U,V) = (7a + \lambda_1 b)U^2 + s + \lambda_1 t$ and $G(U,V) = (7a + \lambda_2 b)U^2 + s + \lambda_2 t$.

From Figure 1 and by Theorem (1), there exists (U,V) in Ω_p^2 such that $F(U,V) = 0$, $G(U,V) = 0$ and $ord_p U = \mu_1$, $ord_p V = \mu_2$ with $\mu_1 = ord_p \frac{s+\lambda_1 t}{7a+\lambda_1 b}$ and $\mu_2 = ord_p \frac{s+\lambda_2 t}{7a+\lambda_2 b}$.

Let $U = \hat{U}$and $V = \hat{V}$. Thus, there exist $(\hat{X} + \hat{x}_0, \hat{Y} + \hat{y}_0)$ in Ω_p^2 such that

$$\hat{U} = \left(\hat{X} + \hat{x}_0\right)^3 + \alpha_1\left(\hat{X} + \hat{x}_0\right)^3\left(\hat{Y} + \hat{y}_0\right)$$

and

$$\hat{V} = \left(\hat{X} + \hat{x}_0\right)^3 + \alpha_2\left(\hat{X} + \hat{x}_0\right)^3\left(\hat{Y} + \hat{y}_0\right)$$

More specifically, $(\hat{X} + \hat{x}_0, \hat{Y} + \hat{y}_0)$ are given by

$$\left(\hat{X} + \hat{x}_0\right) = \left(\frac{\alpha_1 \hat{V} - \alpha_2 \hat{U}}{\alpha_1 - \alpha_2}\right)^{\frac{1}{3}}$$

and

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

with $\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b}$, $\alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b}$ and λ_1, λ_2 are the zeros of $k(\lambda) = \lambda^2 c^2 + bc\lambda + 9b^2 - 35ac$, and $\alpha_1 \neq \alpha_2$ since $\lambda_1 \neq \lambda_2$.

Thus, from Lemma (2.4), we want to find $ord_p \hat{X}$ and $ord_p \hat{Y}$. Therefore, we will consider 2 cases.

i) $ord_p \hat{X} \neq ord_p \hat{x}_0$
ii)$ord_p \hat{X} = ord_p \hat{x}_0$

Considering $ord_p \hat{X} \neq ord_p \hat{x}_0$.
By the properties of

$$ord_p\left(\hat{X} + \hat{x}_0\right) \geq \min\{ord_p \hat{X}, ord_p \hat{x}_0\},$$

it means that

$$ord_p\left(\hat{X} + \hat{x}_0\right) = \min\{ord_p \hat{X}, ord_p \hat{x}_0\} + \varepsilon_1$$

for some $\varepsilon_1 > 0$.

i) Suppose $min = ord_p \hat{X}$, then

$$ord_p \hat{X} + \varepsilon_1 \geq \frac{1}{6}(\alpha - \delta)$$

$$ord_p \hat{X} \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_1$$

ii) Suppose $min = ord_p \hat{x}_0$, then

$$ord_p \hat{x}_0 + \varepsilon_1 \geq \frac{1}{6}(\alpha - \delta)$$

that is

$$ord_p \hat{X} \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_1.$$

Considering $ord_p \hat{X} = ord_p \hat{x}_0$.
i) Suppose $ord_p \hat{X} = ord_p \hat{x}_0 = \omega$, then let

$$\hat{X} = p^\omega m, \qquad ord_p m = 0$$
$$\hat{x}_0 = p^\omega n, \qquad ord_p n = 0$$

Thus

$$ord_p\left(\hat{X} + \hat{x}_0\right) = ord_p(p^\omega m + p^\omega n) = \omega + ord_p(m + n)$$

Let $ord_p(m + n) = \varepsilon_2$, we have,

$$ord_p\left(\hat{X} + \hat{x}_0\right) = \omega + \varepsilon_2 \geq \frac{1}{6}(\alpha - \delta)$$

That is

$$ord_p \hat{X} \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_2.$$

In order to find $ord_p \hat{Y}$, we have to consider 2 cases for both equations : $ord_p\left(\hat{Y} + \hat{y}_0\right) \geq \frac{1}{6}(\alpha - 3\delta)$ or $ord_p\left(\hat{Y} + \hat{y}_0\right) \geq \frac{1}{6}(\alpha - 4\delta)$
i) $ord_p \hat{Y} \neq ord_p \hat{y}_0$
ii) $ord_p \hat{Y} = ord_p \hat{y}_0$

The first cases is in which $ord_p \hat{Y} \neq ord_p \hat{y}_0$.
By the same properties of $ord_p\left(\hat{Y} + \hat{y}_0\right) \geq \min\{ord_p \hat{Y}, ord_p \hat{y}_0\}$, means that

$$ord_p(\hat{Y} + \hat{y}_0) = \min\{ord_p\hat{Y}, ord_p\hat{y}_0\} + \varepsilon_3$$

for some $\varepsilon_3 > 0$.

By using the similar method of finding $ord_p\hat{X}$ and by Lemma (2.4), we will have $ord_p\hat{Y}$ are as follows :

i) Suppose min $= ord_p\hat{Y}$, then

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_3$$

or

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_3$$

or

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_4$$

or

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_4$$

From all cases that we have considered in Lemma (2.4) and suppose $\xi = \hat{X} + \hat{x}_0$ and $\eta = \hat{Y} + \hat{y}_0$, then the results are shown in Table 1 as follows:

$ord_p(\xi - x_0) \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_1$ and	$ord_p(\xi - x_0) \geq \frac{1}{6}(\alpha - \delta) - \varepsilon_2$ and
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 3\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 4\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$ or	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 5\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$ or
$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_3$	$ord_p(\eta - y_0) \geq \frac{1}{6}(\alpha - 6\delta) - \frac{2}{3}\varepsilon_0 - \varepsilon_4$

for some $\varepsilon_0, \varepsilon_2, \varepsilon_4 \geq 0$ and $\varepsilon_1, \varepsilon_3 > 0$.

By back substitution in (12) and (13), we would have $g(\xi, \eta) = f_x(\xi, \eta) = 0$ and $h(\xi, \eta) = f_y(\xi, \eta) = 0$.

Estimation of $N(g, h; p^\alpha)$

Let p be a prime and $g(x, y)$ and $h(x, y)$ are polynomials in $Q_p[x, y]$ and (ξ_i, η_i) are common zeros of g and h. Let $\alpha > 0$ and $H_i(\alpha)$ denote the set $\{(x, y) = \Omega_p^2 : ord_p(x - \xi_i), ord_p(y - \eta_i) = max_j\{ord_p(x - \xi_i), ord_p(y - \eta_i)\} ord_p g(x, y), ord_p h(x, y) \geq \alpha\}$. By using the method of Loxton and Smith (1982), we can show the value of $N(g, h; p^\alpha)$ which can be derived from the sizes of $ord_p(x - \xi_i)$ and $ord_p(y - \eta_i)$ with $(x, y) \in H_i(\alpha)$ for two-variables polynomials as shown by [1],[2]. We state the theorem as follows:

Theorem 3. Let p be a prime and $g(x, y), h(x, y)$ are 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 $N(g, h; p^\alpha) \leq \sum_i p^{2(\alpha > \gamma_i(\alpha))}$.

The next theorem will give the estimate of the cardinality $N(g, h; p^\alpha)$ associated with a polynomial $f(x, y)$ in $Q_p[x, y]$.

Theorem 4. Let $f(x, y) = ax^7 + bx^6y + cx^5y^2 + sx + ty + k$ be a polynomials in $Q_p[x, y]$ with $p > 7$ with p is a prime. Suppose $\alpha > 0$ and $ord_p b^2 \neq ord_p ac$. Let $\delta = \max\{ord_p a, ord_p b, ord_p c\}$, then

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & if \ \alpha \leq \delta \\ 36p^{12\delta + 8\varepsilon_0 + 12q} & if \ \alpha > \delta \end{cases}$$

for some $\varepsilon_0, q \geq 0$ where $q = \max\{\varepsilon_3, \varepsilon_4\}$.

Proof. Clearly, we have $N(f_x, f_y; p^\alpha) \leq p^{2\alpha}$ if $\alpha \leq \delta$.

Now, suppose $\alpha > \delta$. From Theorem (3), we obtain

$$N(f_x, f_y; p^\alpha) \leq \sum_i p^{2(\alpha > \gamma_i(\alpha))}$$

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

From Table 1 and by Theorem 2, we are considering the minimum value of $ord_p(\eta - \hat{y}_0)$ so that we will obtain the upper bound of $N(f_x, f_y; p^\alpha) \leq p^{2\alpha}$ that is,

$$ord_p(\eta - \hat{y}_0) \geq \frac{1}{6}(\alpha - 6\delta) - \frac{2}{3}\varepsilon_0 - q$$

as such

$$\alpha - 6\gamma_i(\alpha) \leq 6\delta + 4\varepsilon_0 + 6q.$$

for $\varepsilon_0, q \geq 0$ where $q = \max\{\varepsilon_3, \varepsilon_4\}$.

By a Theorem of Bezout, the number of common zeros does not exceed the product of the degrees of f_x and f_y.

Therefore,

$$N(f_x, f_y; p^\alpha) \leq 36p^{12\delta+8\varepsilon_0+12q}$$

if$\alpha > \delta$ for $\varepsilon_0, q \geq 0$ where $q = \max\{\varepsilon_3, \varepsilon_4\}$.

Thus, by considering all cases, we have

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & if \ \ \alpha \leq \delta \\ 36p^{12\delta+8\varepsilon_0+12q} & if \ \ \alpha > \delta \end{cases}$$

for some $\varepsilon_0, q \geq 0$ where $q = \max\{\varepsilon_3, \varepsilon_4\}$ as asserted.

CONCLUSION

This cardinality can be used to find the estimation of exponential sums associated with a polynomial of degree seven.

ACKNOWLEDGEMENT

The authors would like to express their gratitude and appreciation for the financial support from MyMaster, Graduate Research Fellowship Grant of Universiti Putra Malaysia and grant FRGS Vot No 5524311 that has enabled them to carry out this research.

REFERENCE

1. MohdAtan, K.A. (1986a). Newton Polyhedra and p-adic Estimate of Zeros of Polynomial in $\Omega_p[x, y]$,Pertanika 9(1), pp. 51-56.

2. MohdAtan, K.A. (1986b).Newton Polyhedral Method of Determining p-adic Orders of Zeros Common to Two Polynomial in $Q_p[x, y]$, Pertanika 9(3), pp. 375-380.

3. MohdAtan, K.A. (1988).A method for Determining the Cardinality of the set of Solutions to Congruence Equations," Pertanika 11(1), pp. 125-131.

4. MohdAtan, K.A. (1995). An Explicit Estimate of Exponential Sums Associated with a Cubic Polynomial," Acta Math. Hungar. 69(1-2), pp. 83-93.

5. Sapar, S. H. and MohdAtan, K.A. (2009).A Method of Estimating the p-adic Sizes of Common Polynomials Associated with a Quintic Form," World Scientific 5(3), pp. 541-554.

6. Yap, H. K., Sapar, S. H. and MohdAtan, K.A. (2011).Estimation of p-adic Sizes of Common Zeros of Partial Derivatives Associated with a Cubic Form," Sains Malaysiana 40(8), pp. 921-926.

7. Aminuddin, S. S., Sapar, S. H. and MohdAtan, K.A. (2013).An Estimating the p-adic Sizes of Common Zeros of Partial Derivative Polynomials," New Trends in Maths Sci. 1(1), pp. 38-48.

8. Aminuddin, S. S., Sapar, S. H. and MohdAtan, K.A. (2014).The Cardinality of the Set of Solutions to Congruence Equation Associated with Cubic Form," JP Journal Algebra, Number Theory and Applications 33(1), pp. 1-23.