ASM Sc. J., 13, 2020
https://doi.org/10.32802/asmscj.2020.sm26(5.14)

# Exponential Sums for Seventh Degree Polynomial

Low Chee Wai[1*], Siti Hasana Sapar[2] and Mohamat Aidil Mohamat Johari[3]

[1,2,3]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia*

[2,3]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia*

Let $f(x,y)$ be a seventh-degree polynomial with two variables in with complete dominant terms. Suppose $p > 7$ is a prime, the exponential sums of polynomial $f(x,y)$ is defined by $S(f;p^\alpha) = \sum_{x,y \bmod p} e^{\frac{2\pi i f(x,y)}{p^\alpha}}$, where the sum is taken over a complete set of residue modulo $p$. In order to get the value of $S(f;p^\alpha)$, the cardinality $N(g,h;p^\alpha)$ must be obtained first. In this paper, we discuss the Newton Polyhedron technique in finding the $p$-adic sizes of common zeros of the partial derivative polynomials $f_x$ and $f_y$ which derive from $f(x,y)$. Then, the estimation of the cardinality and exponential sums of polynomial $f(x,y)$ will be determined accordingly. For $\alpha > 1$, the exponential sums of $f(x,y)$ is given by $|S(f;p^\alpha)| \le \min\{p^{2\alpha}, 36p^{\alpha+1+36\delta+6\omega_0+12q}\}$ where $\delta, \omega_0, q \ge 0$.

**Keywords:** $p$-adic sizes, Newton polyhedron, cardinality, exponential sums

## I. INTRODUCTION

In this paper, $Z_p$ denotes as the field of $p$-adic integer. $\Omega_p$ denotes as the completion of algebraic closure of the field of rational $p$-adic numbers $Q_p$. The highest power of $p$ which divides $x$ is denoted by $ord_p\, x$.

Loxton & Smith (1982) estimated the cardinality $N(f,p^\alpha)$ by the $p$-adic sizes of common zeros of partial derivative polynomials associated with $f$ in the neighborhood of points in the product space $\Omega_p^n$, $n > 0$.

Loxton & Vaughan (1985) studied the estimation of exponential sums by using the number of common zeros of partial derivative polynomials with respect to $x$ modulo $q$.

Mohd. Atan & Loxton (1986) used the Newton polyhedral method to obtain the $p$-adic sizes of polynomials in $\Omega_p[x,y]$ which is an analogue of Newton polygon in Koblitz (1977). They estimated the cardinality for certain lower-degree polynomials $f(x,y)$ over $Z_p$.

The estimations with Newton polyhedron technique for lower degree two-variable polynomials are also found in Mohd. Atan (1986), Chan & Mohd. Atan (1997), Heng & Mohd. Atan (1999) as well as Sapar & Mohd. Atan (2002). However, the results for the higher degree polynomials are less complete.

Then, Sapar & Mohd. Atan (2009) gave the $p$-adic sizes of common zeros of partial derivative polynomials associated with a quintic form for prime $p > 5$.

Yap et al. (2011) showed that the $p$-adic sizes of common zeros of partial derivative polynomials associated with a cubic form can be found explicitly on the indicator diagrams by using Newton polyhedron technique.

Sapar et al. (2013) also investigated the estimation of $p$-adic sizes of common zeros of degree nine polynomial.

Aminudin et al. (2014) continued the research of Yap et al. (2011) on a complete cubic form polynomial. They found that the result is different due to different form of the cubic polynomials. This means different form of polynomials will result different $p$-adic sizes although both of them are cubic polynomials.

Next, Sapar et al. (2014) studied the estimation of $p$-adic sizes of an eighth-degree polynomial. Lasaraiya et al. (2016a) and Lasaraiya et al. (2016b) researched on the

*Corresponding author's e-mail: alexlowcheewai@gmail.com

cardinality $N(f_x, f_y; p^\alpha)$ of twelfth- and eleventh-degree polynomials respectively.

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 $Z_p[x,y]$ of a degree seven. Then, we obtain the estimation of cardinality and the exponential sums of the polynomial

$$f(x,y) = ax^7 + bx^6y + cx^5y^2 + dx^4y^3 + ex^3y^4 + kx^2y^5 + mxy^6 + ny^7 + rx + sy + t.$$

## II. *P*-ADIC SIZE OF COMMON ZERO OF POLYNOMIAL

Sapar & Mohd. Atan (2002) proved that every point of intersection of the Indicator diagrams, there exist common zeros of both polynomials in $Z_p[x,y]$ which $p$-adic sizes correspond to point $(\mu_1, \mu_2)$ as in the following.

**Theorem 1** Let p be a prime. Suppose $f$ and $g$ are polynomials in $Z_p[x,y]$. Let $(\mu_1, \mu_2)$ 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 $\xi$ and $\eta$ in $\Omega_p^2$ satisfying $f(\xi,\eta) = g(\xi,\eta) = 0$ and $ord_p\, \xi = \mu_1, ord_p\, \eta = \mu_2$.

The following theorem gives the $p$-adic size of common zero of polynomial that we consider.

**Theorem 2** Let $f(x,y) = ax^7 + bx^6y + cx^5y^2 + dx^4y^3 + ex^3y^4 + kx^2y^5 + mxy^6 + ny^7 + rx + sy + t$ be a polynomial in $Z_p[x,y]$ and $(x_0, y_0)$ be a point in $\Omega_p^2$ with $p > 7$ is a prime. Let $\alpha > 0$, $\delta = \max\{ord_p a,\ ord_p b,\ ord_p c, ord_p d, ord_p e, ord_p k, ord_p m, ord_p n\}$. 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 $(\xi, \eta)$ such that $f_x(\xi,\eta) = 0,\ f_y(\xi,\eta) = 0$. The $p$-adic sizes are given by

$$ord_p(\xi - x_0) \geq \tfrac{1}{6}(\alpha - 34\delta) - \varepsilon_1,$$

$$ord_p(\eta - y_0) \geq \tfrac{1}{6}(\alpha - 22\delta) - \varepsilon_2$$

for $ord_p(35cn - ek)^2 \neq ord_p 4(21dn - 3em)(5cm - kd)$, and

$$ord_p(\xi - x_0) \geq \tfrac{1}{6}(\alpha - 34\delta) - \varepsilon_3 - \tfrac{1}{2}\omega_0,$$

$$ord_p(\eta - y_0) \geq \tfrac{1}{6}(\alpha - 22\delta) - \varepsilon_4 - \tfrac{1}{2}\omega_0$$

for $ord_p(35cn - ek)^2 = ord_p 4(21dn - 3em)(5cm - kd)$, where $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \omega_0 \geq 0$.

In order to prove Theorem 2, we take a linear combination of $g = f_x(x,y)$ and $h = f_y(x,y)$ as $g + \lambda h$. Then, we do a transformation by letting $U = (X + x_0) + \frac{1}{6}\alpha_1(Y + y_0)$ and $V = (X + x_0) + \frac{1}{6}\alpha_2(Y + y_0)$ where $\alpha_1 = \frac{6b+2\lambda_1 c}{6(7a+\lambda_1 b)}$ and $\alpha_2 = \frac{6b+2\lambda_2 c}{6(7a+\lambda_2 b)}$ that we needed in the following lemma.

**Lemma 1** Let $\lambda_1, \lambda_2$ be the zeros of quadratic function $z(\lambda)$ in the form $z(\lambda) = (21dn - 3em)\lambda^2 + (35cn - ek)\lambda + (5cm - kd)$. Suppose $p$ is a prime and $a, b, c, d, e, k, m, n$ in $Z_p$, then

$$ord_p(\alpha_1 - \alpha_2) = \tfrac{1}{2} ord_p[(35cn - ek)^2 - 4(21dn - 3em)(5cm - kd)] - ord_p(21dn - 3em) + ord_p(14ac - 6b^2) - ord_p(7a + \lambda_1 b) - ord_p(7a + \lambda_2 b).$$

*Proof.* $\alpha_1 - \alpha_2 = \frac{(\lambda_1 - \lambda_2)(14ac - 6b^2)}{6(7a+\lambda_1 b)(7a+\lambda_2 b)}$. Take $ord_p$ on both sides and substitute the expression of $\lambda_1 - \lambda_2 = \frac{\sqrt{(35cn-ek)^2 - 4(21dn-3em)(5cm-kd)}}{(21dn-3em)}$, we obtain:

$$ord_p(\alpha_1 - \alpha_2) = \frac{1}{2} ord_p[(35cn - ek)^2 - 4(21dn - 3em)(5cm - kd)] - ord_p(21dn - 3em) + ord_p(14ac - 6b^2) - ord_p(7a + \lambda_1 b) - ord_p(7a + \lambda_2 b).$$ □

**Lemma 2** Let $p > 7$ be a prime and $a, b, c, d, e, k, m, n, r, s$ in $Z_p$. Suppose $(X + x_0, Y + y_0)$ in $\Omega_p^2$, $\delta = max\{ord_p a,\ ord_p b,\ ord_p c, ord_p d, ord_p e, ord_p k, ord_p m, ord_p n\}$ and $ord_p r, ord_p s \geq \alpha > \delta$.

If $ord_p U = \frac{1}{6} ord_p\left(\frac{r+\lambda_1 s}{7a+\lambda_1 b}\right)$ and $ord_p V = \frac{1}{6} ord_p\left(\frac{r+\lambda_2 s}{7a+\lambda_2 b}\right)$ with the condition $ord_p(35cn - ek)^2 \neq ord_p 4(21dn - 3em)(5cm - kd)$where $= x + \alpha_1 y$ and $V = x + \alpha_2 y$, then

$ord_p(X + x_0) \geq \frac{1}{6}(\alpha - 34\delta)$ and

$ord_p(Y + y_0) \geq \frac{1}{6}(\alpha - 22\delta)$.

*Proof.* Let $x = X + x_0$ and $y = Y + y_0$. Substitute into $U = x + \alpha_1 y$ and $V = x + \alpha_2 y$, we have

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

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

From (2),

$$ord_p(Y + y_0) \geq \min\{ord_p U, ord_p V\} - ord_p(\alpha_1 - \alpha_2). \tag{3}$$

By Lemma 1, we have

$ord_p(Y + y_0)$

$\geq \min\{ord_pU, ord_pV\} - \frac{1}{2}ord_p[(35cn - ek)^2$
$-4(21dn - 3em)\,(5cm - kd)] + ord_p$
$(21dn - 3em) - ord_p(14ac - 6b^2) + ord_p$
$(7a + \lambda_1 b) + ord_p(7a + \lambda_2 b)$.

Since $ord_p(35cn - ek)^2 \neq ord_p 4(21dn - 3em)$ $(5cm - kd)$, we consider two cases.

Case (i): $ord_p(35cn - ek)^2 > ord_p 4(21dn - 3em)(5cm - kd)$,

Case (ii): $ord_p(35cn - ek)^2 < ord_p 4(21dn - 3em)(5cm - kd)$.

For Case (i), equation (3) becomes

$$ord_p(Y + y_0) \geq \min\{ord_pU, ord_pV\} - \frac{1}{2}ord_p(5cm - kd) + \frac{1}{2}ord_p(21dn - 3em) - ord_p(14ac - 6b^2) + ord_p(7a + \lambda_1 b)(7a + \lambda_2 b). \quad (4)$$

We continue with another two cases which are $\min\{ord_pU, ord_pV\} = ord_pU$ and $\min\{ord_pU, ord_pV\} = ord_pV$.

For both cases, we have

$$ord_p(Y + y_0) \geq \frac{1}{6}\min\{ord_pr, ord_p\lambda_i s\} - \frac{1}{2}\min\{ord_pcm, ord_pkd\} - \min\{ord_pac, ord_pb^2\} - \frac{1}{3}\min\{ord_pdn, ord_pem\} \quad (5)$$

where $i = 1, 2$.

By hypothesis, we substitute $\alpha$ and $\delta$, we have

$$ord_p(Y + y_0) \geq \frac{1}{6}(\alpha - 22\delta). \quad (6)$$

For Case (ii), equation (3) becomes

$ord_p(Y + y_0)$
$\geq \min\{ord_pU, ord_pV\} - \frac{1}{2}ord_p(5cm - kd)$
$+\frac{1}{2}ord_p(21dn - 3em) - ord_p(14ac - 6b^2)$
$+ord_p(7a + \lambda_1 b)(7a + \lambda_2 b)$.

It is same as (4). As a result, we will get (6). Now, we need to obtain the $p$-adic size of $(X + x_0)$. By Lemma 1, equation (1) becomes

$ord_p(X + x_0)$

$\geq \min\{ord_p\alpha_1V, ord_p\alpha_2U\} - \frac{1}{2}ord_p[(35cn - ek)^2$
$-4(21dn - 3em)(5cm - kd)] + ord_p$
$(21dn - 3em) - ord_p(14ac - 6b^2) + ord_p$
$(7a + \lambda_1 b) + ord_p(7a + \lambda_2 b). \quad (7)$

Since $ord_p(35cn - ek)^2 \neq ord_p 4(21dn - 3em)$ $(5cm - kd)$, we consider two cases.

Case (iii): $ord_p(35cn - ek)^2 > ord_p 4(21dn - 3em)(5cm - kd)$,

Case (iv): $ord_p(35cn - ek)^2 < ord_p 4(21dn - 3em)(5cm - kd)$.

For Case (iii), equation (7) becomes

$$ord_p(X + x_0) \geq \min\{ord_p\alpha_1V, ord_p\alpha_2U\} - \frac{1}{2}ord_p(5cm - kd) + \frac{1}{2}ord_p(21dn - 3em) - ord_p(14ac - 6b^2) + ord_p(7a + \lambda_1 b)(7a + \lambda_2 b). \quad (8)$$

We continue with another two cases which are $\min\{ord_p\alpha_1V, ord_p\alpha_2U\} = ord_p\alpha_1V$ and $\min\{ord_p\alpha_1V, ord_p\alpha_2U\} = ord_p\alpha_2U$.

For both cases, we obtain

$ord_p(X + x_0) \geq$
$\frac{1}{6}\min\{ord_pr, ord_p\lambda_i s\} - \frac{1}{2}\min\{ord_pcm, ord_pkd\}$
$-\min\{ord_pac, ord_pb^2\} - \frac{4}{3}\min\{ord_pdn, ord_pem\}$

where $i = 1, 2$.

By hypothesis, we obtain

$$ord_p(X + x_0) \geq \frac{1}{6}(\alpha - 34\delta). \quad (9)$$

For Case (iv), equation (7) becomes

$ord_p(X + x_0) \geq$
$\min\{ord_p\alpha_1V, ord_p\alpha_2U\} - \frac{1}{2}ord_p[4(21dn - 3em)$
$(5cm - kd)] + ord_p(21dn - 3em) - ord_p$
$(14ac - 6b^2) + ord_p(7a + \lambda_1 b) + ord_p(7a + \lambda_2 b)$.

That is,

$$ord_p(X + x_0) \geq \min\{ord_p\alpha_1V, ord_p\alpha_2U\} - \frac{1}{2}ord_p + ord_p(5cm - kd) + \frac{1}{2}ord_p(21dn - 3em) - ord_p(14ac - 6b^2) + ord_p(7a + \lambda_1 b)(7a + \lambda_2 b).$$

It is same as (8). As a result, we will get (9). □

In order to see the validity of our result and by Bezout's Theorem, we have $\alpha > (n-1)^2\delta$. Then, we have $\alpha > 36\delta$ in which $\alpha - 36\delta$ is the minimum value that we can get. In Lemma 2, we have $\alpha - 34\delta$ and $\alpha - 22\delta$ are greater than the minimum value. Thus, our lemma is valid.

**Lemma 3** Let $p > 7$ be a prime and $a, b, c, d, e, k, m, n, r, s$ in $Z_p$. Suppose $(X + x_0, Y + y_0)$ in $\Omega_p^2$, $\delta = max\{ord_pa,\ ord_pb,\ ord_pc, ord_pd, ord_pe, ord_pk, ord_pm, ord_pn\}$ and $ord_pr, ord_ps \geq \alpha > \delta$.

If $ord_pU = \frac{1}{6}ord_p\left(\frac{r+\lambda_1 s}{7a+\lambda_1 b}\right)$ and $ord_pV = \frac{1}{6}ord_p\left(\frac{r+\lambda_2 s}{7a+\lambda_2 b}\right)$ with the condition $ord_p(35cn-ek)^2 = ord_p4(21dn-3em)(5cm-kd)$ where $U = x+\alpha_1 y$ and $V = x+\alpha_2 y$, then $ord_p(X+x_0) \geq \frac{1}{6}(\alpha-34\delta)-\frac{1}{2}\omega_0$ and $ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-22\delta)-\frac{1}{2}\omega_0$ for some $\omega_0 \geq 0$.

*Proof.* From Lemma 2, we have

$$ord_p(Y+y_0) \geq \min\{ord_pU, ord_pV\} - \frac{1}{2}ord_p[(35cn-ek)^2 -4(21dn-3em)(5cm-kd)] + ord_p(21dn-3em) - ord_p(14ac-6b^2) + ord_p(7a+\lambda_1 b) +ord_p(7a+\lambda_2 b).$$

If $\min\{ord_pU, ord_pV\} = ord_pU$, then we obtain

$$ord_p(Y+y_0) \geq \frac{1}{6}ord_p\left(\frac{r+\lambda_1 s}{7a+\lambda_1 b}\right) - \frac{1}{2}ord_p[(35cn-ek)^2-4(21dn-3em)(5cm-kd)] + ord_p(21dn-3em) - ord_p(14ac-6b^2) + ord_p(7a+\lambda_1 b)+ord_p(7a+\lambda_2 b).$$

Now, let $ord_p(35cn-ek)^2 = ord_p4(21dn-3em)(5cm-kd) = \gamma$, we have $(35cn-ek)^2 = Ap^\gamma$ and $4(21dn-3em)(5cm-kd) = Bp^\gamma$ where $ord_pA = ord_pB = 0$. Then,

$$ord_p[(35cn-ek)^2 - 4(21dn-3em)(5cm-kd)] = ord_p(Ap^\gamma - Bp^\gamma) = \gamma + \omega_0$$

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

Now, we choose $\gamma = ord_p4(21dn-3em)(5cm-kd)$ and substitute the expression of $\lambda_1, \lambda_2$. Then,

$$ord_p(Y+y_0) \geq \frac{1}{6}ord_p(r+\lambda_1 s) - \frac{1}{2}ord_p(5cm-kd) - \frac{1}{3}ord_p(21dn-3em) - ord_p(14ac-6b^2) - \frac{1}{2}\omega_0.$$

By using the hypothesis, we have

$$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-22\delta) - \frac{1}{2}\omega_0$$

for some $\omega_0 \geq 0$.

If $\min\{ord_pU, ord_pV\} = ord_pV$, then we obtain

$$ord_p(Y+y_0) \geq \frac{1}{6}ord_p\left(\frac{r+\lambda_2 s}{7a+\lambda_2 b}\right) - \frac{1}{2}ord_p[(35cn-ek)^2 -4(21dn-3em)(5cm-kd)] + ord_p(21dn-3em) - ord_p(14ac-6b^2) + ord_p(7a+\lambda_1 b) +ord_p(7a+\lambda_2 b).$$

By substituting the expression of $\lambda_1, \lambda_2$ and using the hypothesis, we have

$$ord_p(Y+y_0) \geq \frac{1}{6}(\alpha-22\delta) - \frac{1}{2}\omega_0$$

for some $\omega_0 \geq 0$.

Also, from Lemma 2, we have

$$ord_p(X+x_0) \geq \min\{ord_p\alpha_1 V, ord_p\alpha_2 U\} - \frac{1}{2}ord_p[(35cn-ek)^2 -4(21dn-3em)(5cm-kd)] + ord_p(21dn-3em) - ord_p(14ac-6b^2) + ord_p(7a+\lambda_1 b) +ord_p(7a+\lambda_2 b).$$

If $\min\{ord_p\alpha_1 V, ord_p\alpha_2 U\} = ord_p\alpha_1 V$. By using the same argument, we obtain

$$ord_p(X+x_0) \geq \frac{1}{6}ord_p(r+\lambda_2 s) - \frac{1}{2}ord_p(5cm-kd) - \frac{4}{3}ord_p(21dn-3em) - ord_p(14ac-6b^2) - \frac{1}{2}\omega_0.$$

For the case $\min\{ord_p\alpha_1 V, ord_p\alpha_2 U\} = ord_p\alpha_2 U$. By using the similar manner, we have

$$ord_p(X+x_0) \geq \frac{1}{6}ord_p(r+\lambda_1 s) - \frac{1}{2}ord_p(5cm-kd) - \frac{4}{3}ord_p(21dn-3em) - ord_p(14ac-6b^2) - \frac{1}{2}\omega_0.$$

By hypothesis, we have the following result:

$$ord_p(X+x_0) \geq \frac{1}{6}(\alpha-34\delta) - \frac{1}{2}\omega_0$$

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

Now, we will prove the Theorem 2.

*Proof of Theorem 2.*

Let $g = f_x$ and $h = f_y$. Suppose $x = X+x_0$ and $y = Y+y_0$. By completing the sixth degree,

$$\frac{g+\lambda h}{7a+\lambda b} = \left[(X+x_0) + \frac{1}{6}\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)(Y+y_0)\right]^6 + \left(\frac{r+\lambda s}{7a+\lambda b}\right) \quad (10)$$

with

$$\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)^2 - \frac{36}{15}\left(\frac{5c+3\lambda d}{7a+\lambda b}\right) = 0 \quad (11)$$

$$\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)^3 - \frac{54}{5}\left(\frac{4d+4\lambda e}{7a+\lambda b}\right) = 0 \quad (12)$$

$$\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)^4 - \frac{432}{5}\left(\frac{3e+5\lambda k}{7a+\lambda b}\right) = 0 \quad (13)$$

$$\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)^5 - 6^4\left(\frac{2k+6\lambda m}{7a+\lambda b}\right) = 0 \quad (14)$$

$$\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)^6 - 6^6\left(\frac{m+7\lambda n}{7a+\lambda b}\right) = 0. \quad (15)$$

By solving (11), (12), (13), (14) and (15) simultaneously, we obtain a quadratic equation

$$(21dn-3em)\lambda^2 + (35cn-ek)\lambda + (5cm-kd) = 0.$$

Let

$$U = (X + x_0) + \frac{1}{6}\left(\frac{6b + 2\lambda_1 c}{7a + \lambda_1 b}\right)(Y + y_0) \qquad (16)$$

$$V = (X + x_0) + \frac{1}{6}\left(\frac{6b + 2\lambda_2 c}{7a + \lambda_2 b}\right)(Y + y_0), \qquad (17)$$

we have

$$g + \lambda_1 h = (7a + \lambda_1 b)U^6 + r + \lambda_1 s \qquad (18)$$

$$g + \lambda_2 h = (7a + \lambda_2 b)V^6 + r + \lambda_2 s. \qquad (19)$$

We let $F(U,V) = g + \lambda_1 h$ and $G(U,V) = g + \lambda_2 h$.

The combination of the indicator diagrams associated with the Newton polyhedron of (18) and (19) as shown in Figure 1. There exists a point $(U,V)$ such that $F(U,V) = 0$ and $G(U,V) = 0$ where $(\mu_1, \mu_2)$ is the point of intersection in the indicator diagrams of $F(U,V)$ and $G(U,V)$.

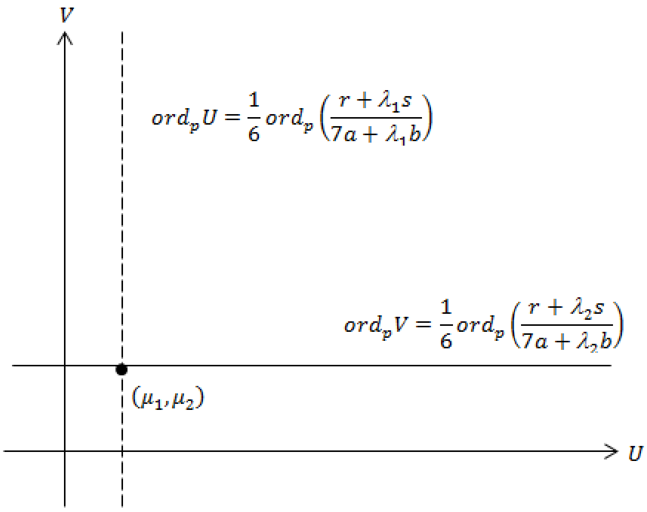


Figure 1. The indicator diagrams for the polynomials of $F(U,V)$ (dash line) and $G(U,V)$ (solid line).

Let $U = \hat{U}$ and $V = \hat{V}$. From (16) and (17), there exists $(\hat{X} + \hat{x}_o)$ and $(\hat{Y} + \hat{y}_o)$ 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 $\alpha_1 = \frac{6b+2\lambda_1 c}{6(7a+\lambda_1 b)}$, $\alpha_2 = \frac{6b+2\lambda_2 c}{6(7a+\lambda_2 b)}$ and $\lambda_1, \lambda_2$ are the zeros of $z(\lambda)$ in Lemma 1. Next, we find $ord_p\hat{X}$ and $ord_p\hat{Y}$. From Lemma 2, we have

$$ord_p(\hat{X} + \hat{x}_0) \geq \frac{1}{6}(\alpha - 34\delta),$$

$$ord_p(\hat{Y} + \hat{y}_0) \geq \frac{1}{6}(\alpha - 22\delta).$$

By the following property,

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

$$ord_p(\hat{X} + \hat{x}_0) \geq ord_p\hat{X} + \varepsilon_1$$

$$ord_p(\hat{Y} + \hat{y}_0) \geq ord_p\hat{Y} + \varepsilon_2$$

for some $\varepsilon_1, \varepsilon_2 \geq 0$. Thus, we will have

$$ord_p\hat{X} \geq \frac{1}{6}(\alpha - 34\delta) - \varepsilon_1,$$

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 22\delta) - \varepsilon_2.$$

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

$$ord_p(\xi - \hat{x}_o) \geq \frac{1}{6}(\alpha - 34\delta) - \varepsilon_1,$$

$$ord_p(\eta - \hat{y}_o) \geq \frac{1}{6}(\alpha - 22\delta) - \varepsilon_2.$$

By back substitution, we have

$g(\xi, \eta) = f_x(\xi, \eta) = 0$ and $h(\xi, \eta) = f_y(\xi, \eta) = 0$.

From Lemma 3, we have

$$ord_p(\hat{X} + \hat{x}_o) \geq \frac{1}{6}(\alpha - 34\delta) - \frac{1}{2}\omega_o$$

$$ord_p(\hat{Y} + \hat{y}_o) \geq \frac{1}{6}(\alpha - 22\delta) - \frac{1}{2}\omega_o.$$

By the same property, we have

$$ord_p(\hat{X} + \hat{x}_0) \geq ord_p\hat{X} + \varepsilon_3$$

$$ord_p(\hat{Y} + \hat{y}_0) \geq ord_p\hat{Y} + \varepsilon_4$$

for some $\varepsilon_3, \varepsilon_4 \geq 0$. Thus, we will obtain

$$ord_p\hat{X} \geq \frac{1}{6}(\alpha - 34\delta) - \varepsilon_3 - \frac{1}{2}\omega_0,$$

$$ord_p\hat{Y} \geq \frac{1}{6}(\alpha - 22\delta) - \varepsilon_4 - \frac{1}{2}\omega_0.$$

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

$$ord_p(\xi - \hat{x}_o) \geq \frac{1}{6}(\alpha - 34\delta) - \varepsilon_3 - \frac{1}{2}\omega_0,$$

$$ord_p(\eta - \hat{y}_0) \geq \frac{1}{6}(\alpha - 22\delta) - \varepsilon_4 - \frac{1}{2}\omega_0.$$

By back substitution, we have

$g(\xi, \eta) = f_x(\xi, \eta) = 0$ and $h(\xi, \eta) = f_y(\xi, \eta) = 0$. □

## III. ESTIMATION OF CARDINALITY $N(f_x, f_y; p^\alpha)$

From Loxton & Smith (1982), we can get the $N(f_x, f_y; p^\alpha)$ from the $p$-adic size of $ord_p(x - \xi_i)$ 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 $\alpha > 0$, $(\xi_i, \eta_i)$, $i \geq 0$ be common zeros of $g$ and $h$, and $\gamma_i(\alpha) = \inf_{x \in H(\alpha)}\{ord_p(x - \xi_i), ord_p(y - \eta_i)\}$ where $H(\alpha) = \cup_i H_i(\alpha)$. If $\alpha > \gamma_i(\alpha)$, then $N(g, h; p^\alpha) \leq \sum_i p^{2(\alpha - \gamma_i(\alpha))}$.

Next, we can prove the following theorem.

**Theorem 4** Let $f(x,y) = ax^7 + bx^6y + cx^5y^2 + dx^4y^3 + ex^3y^4 + kx^2y^5 + mxy^6 + ny^7 + rx + sy + t$ be a polynomial in $Z_p[x,y]$ with $p > 7$ is a prime. Let $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b, ord_p c,$

$ord_p d, ord_p e, ord_p k, ord_p m, ord_p n\}$, then

$$N(f_x, f_y; p^\alpha) \leq \begin{cases} p^{2\alpha} & if\ \alpha \leq \delta \\ 36p^{68\delta+12q} & if\ \alpha > \delta \end{cases}$$

where $q = \max\left\{\varepsilon_1,\ \varepsilon_3 + \frac{1}{2}\omega_0\right\}$.

*Proof.* If $\alpha \leq \delta$, then $N(f_x, f_y; p^\alpha) \leq p^{2\alpha}$ since $\gamma_i(\alpha) = 0$. If $\alpha > \delta$, from Theorem 3, we have

$$ord_p(\xi - x_0) \geq \frac{1}{6}(\alpha - 34\delta) - q$$

where $q = \max\left\{\varepsilon_1,\ \varepsilon_3 + \frac{1}{2}\omega_0\right\}$. We obtain

$$\alpha - 6\gamma_i(\alpha) \leq 34\delta + 6q.$$

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

$$N(f_x, f_y; p^\alpha) \leq 36p^{68\delta+12q}$$

for $\alpha > \delta$ and $q = \max\left\{\varepsilon_1,\ \varepsilon_3 + \frac{1}{2}\omega_0\right\}$. □

## IV. ESTIMATION OF EXPONENTIAL SUMS $S(f; p^\alpha)$

The exponential sums can be estimated by using the theorems in Mohd. Atan (1984).

**Theorem 5** Let $p$ be a prime and $f(x,y)$ be a polynomial in $Z_p[x,y]$. For $\alpha > 1$, $\theta = \frac{\alpha}{2}$, let

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

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

If $\alpha$ is odd, then we use the next theorem.

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

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

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

$$|S(f; p^\alpha)| \leq \min\{p^{2\alpha}, 36p^{\alpha+1+68\delta+12q}\}$$

where $q = \max\left\{\varepsilon_1,\ \varepsilon_3 + \frac{1}{2}\omega_0\right\}$.

*Proof.* From Theorem 4, we have

$$N(f_x, f_y; p^\alpha) \leq \min\{p^{2\alpha}, 36p^{68\delta+12q}\}$$

where $\theta = \frac{\alpha}{2}$ and $q = \max\left\{\varepsilon_1,\ \varepsilon_3 + \frac{1}{2}\omega_0\right\}$.

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

$$|S(f; p^\alpha)| \leq \min\{p^{2\alpha}, 36p^{\alpha+68\delta+12q}\}.$$

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

$$|S(f; p^\alpha)| \leq \min\{p^{2\alpha}, 36p^{\alpha+1+68\delta+12q}\}.$$ □

## V. CONCLUSION

The exponential sums of the seventh-degree polynomial with two variables in the form

$$f(x,y) = ax^7 + bx^6y + cx^5y^2 + dx^4y^3 + ex^3y^4$$
$$+kx^2y^5 + mxy^6 + ny^7 + rx + sy + t$$

in $Z_p[x,y]$ is given by

$$|S(f; p^\alpha)| \leq \min\{p^{2\alpha}, 36p^{\alpha+1+68\delta+12q}\}$$

where $p, q, \alpha$ and $\delta$ are defined in Theorem 7.

## VI. ACKNOWLEDGEMENT

We take this opportunity to express our gratitude for the financial support from Graduate Research Fellowship of UPM, grant UPM/700-2/1/GBP/2017/9597900 and those helps in this research to make it success.

## VII. REFERENCES


Aminudin, S. S., Sapar, S. H. & 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. International Conference on Mathematical Sciences and Statistics 2013, 205-212.

Chan, K. L. & 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. & Mohd. Atan, K. A. (1999). An estimation of exponential sums associated with a cubic form. J. Phys. Sci., 10, 1-21.

Koblitz, N. (1977). p-adic Numbers, p-adic Analysis and Zeta-Functions. New York, Second Edition (Springer-Verlag), 89-99.

Lasaraiya, S., Sapar, S. H. & Johari, M. A. M. (2016a). On the cardinality of the twelfth-degree polynomial. In AIP Conference Proceedings, 020008, AIP Publishing.

Lasaraiya, S., Sapar, S. H. & Johari, M. A. M. (2016b). On the cardinality of the set of solutions to congruence equation associated with polynomial of degree eleven. In P Conference Proceedings, 050015, AIP Publishing.

Loxton, J. H. & Smith, R. A. (1982). Estimate for multiple exponential sums. J. Aust. Math. Soc., 33, 125-134.

Loxton, J. H. & Vaughan, R. C. (1985). The estimate of complete exponential sums. Canad. Math. Bull., 28(4), 440-454.

Mohd. Atan, K. A. (1984). Newton polyhedral and estimates for exponential sums. Ph.D. Thesis, University of New South Wales, Kensington, Australia.

Mohd. Atan, K. A. & Loxton, J. H. (1986). Newton Polyhedra and Solutions of Congruences. In Proceeding of Diophantine Analysis, Cambridge University Press, 67-82.

Mohd. Atan, K. A. (1986). Newton polyhedral method of determining p-adic orders of zeros common to two polynomials in $Q_p[x, y]$. Pertanika, 9(3), 375-380.

Sapar, S. H. & Mohd. Atan, K. A. (2002). Estimate for the cardinality of the set of solution to congruence equations. J. Technology, 36(C), 13-40.

Sapar, S. H. & 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. World Scientific, 5, 541-554.

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

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

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