

A Method of Estimating the p -adic Sizes of Common Zeros of Partial Derivative Polynomials Associated with an n^{th} Degree Form

¹Sapar S.H. & ²Mohd Atan K.A.

¹Mathematics Department, Faculty of Science

²Laboratory of Theoretical Mathematics, Institute for Mathematical Research,
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
E-mail: ¹sitihas@fsas.upm.edu.my ; ²kamel@putra.upm.edu.my

ABSTRACT

Let $\underline{x} = (x_1, x_2, \dots, x_n)$ be a vector in a space Z^n where Z is the ring of integers and let q be a positive integer, f a polynomial in \underline{x} with coefficients in Z . The exponential sum associated with f is defined as

$$S(f; q) = \sum \exp(2\pi i f(x)/q)$$

where the sum is taken over a complete set of residues modulo q .

The value of $S(f; q)$ has been shown to depend on the estimate of the cardinality $|V|$, the number of elements contained in the set

$$V = \{\underline{x} \bmod q \mid \underline{f}_{\underline{x}} \equiv \underline{0} \bmod q\}$$

where $\underline{f}_{\underline{x}}$ is the partial derivatives of f with respect to \underline{x} . To determine the cardinality of V , the information on the p -adic sizes of common zeros of the partial derivatives polynomials need to be obtained.

This paper discusses a method of determining the p -adic sizes of the components of (ξ, η) , a common root of partial derivatives polynomial of $f(x, y)$ in of degree n , where n is odd based on the p -adic Newton polyhedron technique associated with the polynomial. The polynomial of degree n is of the form

$$f(x, y) = ax^n + bx^{n-1}y + cx^{n-2}y^2 + sx + ty + k$$

Keywords: Exponential sums, Cardinality, p -adic sizes, Newton polyhedron 2000
Mathematics Subject Classification: 11D45 ; 11T23

INTRODUCTION

In this paper, the notations Z_p , Ω_p and $ord_p x$ are used to denote the ring of p -adic integers, completion of the algebraic closure \mathcal{Q}_p the field of rational p -adic numbers and the highest power of p , which divides x . For each prime p , let $\underline{f} = (f_1, f_2, \dots, f_n)$ be an n -tuple polynomials in $Z_p[\underline{x}]$, where Z_p is the ring of p -adic integers and $\underline{x} = (x_1, x_2, \dots, x_n)$.

The estimation of $|V|$ has been the subject of many research in number theory, one of which is in finding the best possible estimate to multiple exponential sums of the form

$$S(f; q) = \sum_{x \bmod q} \exp\left(\frac{2\pi i f}{q}\right) \text{ where } f(\underline{x}) \text{ is a polynomial in } Z[\underline{x}] \text{ and the sum is taken}$$

over a complete set of residues x modulo a positive integer q .

Loxton and Vaughn (1985) are among the researchers who investigated $S(f; q)$ where f is a non-linear polynomial in $Z[\underline{x}]$. They found that the estimate of $S(f; q)$ depends on the value of $|V|$, the number of common zeros of the partial derivatives of f with respect to \underline{x} modulo q . By using this result, the estimate of $S(f; q)$ was found by other researchers such as Mohd Atan (1986). He considered in particular the non-linear polynomial

$$f(x, y) = ax^3 + bx^2y + cx + dy + e. \text{ He found that the } p\text{-adic sizes for the zero}$$

$$(\xi, \eta) \text{ of this polynomial is } \text{ord}_p \xi \geq \frac{1}{2}(\alpha - \delta) \text{ and } \text{ord}_p \eta \geq \frac{1}{2}(\alpha - \delta) \text{ with}$$

$$\delta = \max\left\{\text{ord}_p 3a, \frac{3}{2}\text{ord}_p b\right\}.$$

Mohd Atan and Abdullah (1992) considered a cubic polynomial of the form

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + kx + my + n$$

and obtained the p -adic sizes for the root (ξ, η) of this polynomial as $\text{ord}_p \xi \geq \frac{1}{2}(\alpha - \delta)$

and $\text{ord}_p \eta \geq \frac{1}{2}(\alpha - \delta)$ with $\delta = \max\{\text{ord}_p 3a, \text{ord}_p b, \text{ord}_p c, \text{ord}_p 3d\}$.

Chan and Mohd Atan (1997) investigated a polynomial of a higher degree than the one considered above in $Z_p[x, y]$ of the form

$$f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 + mx + ny + k$$

and showed that for a root (ξ, η) of $f(x, y)$, the p -adic sizes for the zero (ξ, η) of this

polynomial is $\text{ord}_p \xi \geq \frac{1}{3}(\alpha - \delta)$ and $\text{ord}_p \eta \geq \frac{1}{3}(\alpha - \delta)$ with

$$\delta = \max\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p c, \text{ord}_p d, \text{ord}_p e\}.$$

Heng and Mohd Atan (1999) determined the cardinality associated with the partial derivatives functions of the cubic form

$$f(x,y)=ax^3+bx^2y+cx+dy+e$$

In their work, they attempted to find a better estimate by looking at the maximum number of common zeros associated with the partial derivatives $f_x(x,y)$ and $f_y(x,y)$. A sharper result was obtained with δ similar to the one considered by Mohd Atan (1986). However, the general result for polynomials of several variables is less complete.

In this paper, a method of determining the p -adic sizes of the component (ξ,η) a common root of partial polynomial of $f(x,y)$ in of degree n where n is odd is discussed. The polynomial considered in this paper is of the form

$$f(x,y)=ax^n+bx^{n-1}y+cx^{n-2}y^2+sx+ty+k.$$

The desired estimate is arrived at by examining the combinations of the indicator diagrams associated with the Newton polyhedrons of f_x and f_y developed by Mohd Atan and Loxton (1986). It is an analogue of the p -adic Newton polygon developed by Koblitz (1977).

p-adic Orders of Zeros of a Polynomial

Mohd Atan and Loxton (1986) conjectured that to every point of intersection of the combination of the indicator diagrams associated with the Newton polyhedrons of a pair of polynomials in $Z_p[x,y]$, there exist common zeros of both polynomials whose p -adic orders correspond to this point. The conjecture is as follows :

- Conjecture

Let p be a prime. Suppose f and g are polynomials in $Z_p[x,y]$. Let (μ,λ) be a point of intersection of the indicator diagrams associated with f and g . Then there are ξ and η in Ω_p satisfying $f(\xi,\eta)=g(\xi,\eta)=0$ and $ord_p \xi=\mu$, $ord_p \eta=\lambda$.

A special case of this conjecture was proved by Mohd Atan and Loxton (1986). Sapar and Mohd Atan (2002) improved on this result as follows:

Theorem 2.1

Let p be a prime. Suppose f and g are polynomials in $Z_p[x,y]$. Let (μ,λ) be a point of intersection of the indicator diagrams associated with f and g at the vertices or simple points of intersections. Then there are ξ and η in Ω_p satisfying $f(\xi,\eta)=g(\xi,\eta)=0$ and $ord_p \xi=\mu$, $ord_p \eta=\lambda$.

In Theorems 2.5 and 2.6 that follow, the p -adic sizes of common zeros of partial derivatives of the polynomial $f(x, y) = ax^n + bx^{n-1}y + cx^{n-2}y^2 + sx + ty + k$ where n is odd are given. First, the the following assertions are made

Lemma 2.1

Let $n > 1$ be a positive integer and $p > n$ be a prime. Let a, b, c, s and t be in Z_p and λ_1, λ_2 are the zeros of $h(\lambda) = 4c^2\lambda^2 + 4bc\lambda + (n-1)^2b^2 - 4n(n-2)ac$ and let

$$\alpha_1 = \frac{(n-1)b + 2\lambda_1c}{2(na + \lambda_1b)} \quad \text{and} \quad \alpha_2 = \frac{(n-1)b + 2\lambda_2c}{2(na + \lambda_2b)}$$

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

$$\text{ord}_p (\alpha_1 + \alpha_2) = \text{ord}_p \frac{b}{a}.$$

Proof:

$$\lambda_1 = \frac{-b + \sqrt{n(n-2)(4ac - b^2)}}{2c} \quad \text{and} \quad \lambda_2 = \frac{-b - \sqrt{n(n-2)(4ac - b^2)}}{2c}$$

are the zeros of $h(\lambda) = 4c^2\lambda^2 + 4bc\lambda + (n-1)^2b^2 - 4n(n-2)ac$. Then

$$\lambda_1c = \frac{-b + \sqrt{n(n-2)(4ac - b^2)}}{2}$$

Since $\text{ord}_p b^2 > \text{ord}_p ac$ and $p > n$, we have

$$\text{ord}_p \sqrt{n(n-2)(4ac - b^2)} = \frac{1}{2} \text{ord}_p ac$$

Hence, $\text{ord}_p \left(-b + \sqrt{n(n-2)(4ac - b^2)} \right) = \frac{1}{2} \text{ord}_p ac$

Thus, $\text{ord}_p 2\lambda_1c = \frac{1}{2} \text{ord}_p ac < \text{ord}_p b$.

By the same method, it can be shown that

$$\text{ord}_p 2\lambda_2c = \frac{1}{2} \text{ord}_p ac < \text{ord}_p b.$$

Therefore,

$$\text{ord}_p ((n-1)b + 2\lambda_i c) = \text{ord}_p 2\lambda_i c = \frac{1}{2} \text{ord}_p ac, \quad i = 1, 2. \tag{1}$$

Consider that

$$\lambda_1 b = b \left[\frac{-b + \sqrt{n(n-2)(4ac - b^2)}}{2c} \right]$$

Then,

$$\text{ord}_p \lambda_1 b = \text{ord}_p b + \text{ord}_p [-b + \sqrt{n(n-2)(4ac - b^2)}] - \text{ord}_p 2c$$

Since $\text{ord}_p b > \frac{1}{2} \text{ord}_p ac$ and $p > n$, we have

$$\begin{aligned} \text{ord}_p \lambda_1 b &= \text{ord}_p b + \frac{1}{2} \text{ord}_p ac - \text{ord}_p c \\ &> \frac{1}{2} \text{ord}_p ac + \frac{1}{2} \text{ord}_p ac - \text{ord}_p c \\ &= \text{ord}_p a. \end{aligned}$$

Thus, $\text{ord}_p \lambda_1 b > \text{ord}_p a$

Again by the same method, we can show that

$$\text{ord}_p \lambda_2 b > \text{ord}_p a$$

Therefore, we obtain that

$$\text{ord}_p 2(na + \lambda_i b) = \text{ord}_p a, i = 1, 2 \quad (2)$$

From (1) and (2),

$$\begin{aligned} \text{ord}_p \alpha_i &= \text{ord}_p \left(\frac{(n-1)b + 2\lambda_i c}{2(na + \lambda_i b)} \right), i = 1, 2 \\ &= \frac{1}{2} \text{ord}_p ac - \text{ord}_p a \end{aligned}$$

That is, $\text{ord}_p \alpha_i = \frac{1}{2} \text{ord}_p \frac{c}{a}, i = 1, 2 \quad (3)$

It can be shown that

$$\alpha_1 - \alpha_2 = \frac{(\lambda_1 - \lambda_2)(2nac - (n-1)b^2)}{2(na + \lambda_1 b)(na + \lambda_2 b)}$$

with $\lambda_1 - \lambda_2 = \frac{\sqrt{n(n-2)(4ac-b^2)}}{c}$

Then,

$$\begin{aligned} \text{ord}_p(\alpha_1 - \alpha_2) &= \text{ord}_p \sqrt{n(n-2)(4ac-b^2)} - \text{ord}_p c + \text{ord}_p(2nac - (n-1)b^2) \\ &\quad - \text{ord}_p 2(na + \lambda_1 b) - \text{ord}_p(na + \lambda_2 b) \end{aligned}$$

Since $p > n$, $\text{ord}_p b^2 > \text{ord}_p ac$ and from (2), we have

$$\begin{aligned} \text{ord}_p(\alpha_1 - \alpha_2) &= \frac{1}{2} \text{ord}_p ac - \text{ord}_p c + \text{ord}_p ac - 2\text{ord}_p a \\ &= \frac{1}{2} (\text{ord}_p c - \text{ord}_p a) \end{aligned}$$

That is, $\text{ord}_p(\alpha_1 - \alpha_2) = \frac{1}{2} \left(\text{ord}_p \frac{c}{a} \right)$ (4)

From (3) and (4), we obtain

$$\text{ord}_p \alpha_i = \text{ord}_p(\alpha_1 - \alpha_2) = \frac{1}{2} \text{ord}_p \frac{c}{a}, \quad i = 1, 2.$$

Also, its can be shown that

$$\alpha_1 + \alpha_2 = \frac{[2n(n-1)ab + 4bc\lambda_1\lambda_2 + (2nac + (n-1)b^2)(\lambda_1 + \lambda_2)]}{2(na + \lambda_1 b)(na + \lambda_2 b)}$$

with $\lambda_1\lambda_2 = \frac{(1-n)^2 b^2 - 4n(n-2)ac}{4c^2}$ and $\lambda_1 + \lambda_2 = -\frac{b}{c}$.

Then

$$\begin{aligned} \text{ord}_p(\alpha_1 + \alpha_2) &= \text{ord}_p \frac{2b}{c} ((2-n)(1+n)b^2 + 6n(n-2)ac) \\ &\quad - \text{ord}_p 2(na + \lambda_1 b) - \text{ord}_p(na + \lambda_2 b) \end{aligned}$$

Since $p > n$, $\text{ord}_p b^2 > \text{ord}_p ac$ and from (2), we have

$$\begin{aligned} \text{ord}_p (\alpha_1 + \alpha_2) &= \text{ord}_p \frac{b}{c} + \text{ord}_p ac - 2\text{ord}_p a \\ &= \text{ord}_p \frac{b}{a} \end{aligned}$$

Therefore, we obtain

$$\text{ord}_p \alpha_i = \text{ord}_p (\alpha_1 - \alpha_2) = \frac{1}{2} \text{ord}_p \frac{c}{a}, \text{ bagi } i = 1, 2$$

and $\text{ord}_p (\alpha_1 + \alpha_2) = \text{ord}_p \frac{b}{a}$ as asserted.

In the Lemma 2.2 and Theorem 2.2,

$$\alpha_1 = \frac{(n-1)b + 2\lambda_1 c}{2(na + \lambda_1 b)}, \alpha_2 = \frac{(n-1)b + 2\lambda_2 c}{2(na + \lambda_2 b)} \text{ where } \lambda_1, \lambda_2 \text{ are the zeros of}$$

$h(\lambda) = 4c^2 \lambda^2 + 4bc\lambda + (n-1)^2 b^2 - 4n(n-2)ac$. Then $\alpha_1 \neq \alpha_2$ because of

$$\lambda_1 \neq \lambda_2.$$

Lemma 2.2

Suppose U, V in $\Omega_p \times \Omega_p$. Let $n > 1$ be a positive integer and $p > n$ be a prime, a, b and c in Z_p .

If $\text{ord}_p b^2 > \text{ord}_p ac$, then

$$\text{ord}_p (\alpha_1 V - \alpha_2 U) = \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] - \text{ord}_p a.$$

Proof

$$\begin{aligned} \text{ord}_p (\alpha_1 V - \alpha_2 U) &= \text{ord}_p \left(\frac{(n-1)b + 2\lambda_1 c}{2(na + \lambda_1 b)} V - \frac{(n-1)b + 2\lambda_2 c}{2(na + \lambda_2 b)} U \right) \\ &= \text{ord}_p \left[[(n-1)b + 2\lambda_1 c](na + \lambda_2 b)V - [(n-1)b + 2\lambda_2 c](na + \lambda_1 b)U \right] \\ &\quad - \text{ord}_p 2(na + \lambda_1 b) - \text{ord}_p 2(na + \lambda_2 b) \end{aligned} \tag{1}$$

Now,

$$\lambda_1 = \frac{-b + \sqrt{n(n-2)(4ac-b^2)}}{2c} \text{ and } \lambda_2 = \frac{-b - \sqrt{n(n-2)(4ac-b^2)}}{2c}$$

are the zeros of $h(\lambda) = 4c^2\lambda^2 + 4bc\lambda + (n-1)^2b^2 - 4n(n-2)ac$.
 It can be shown that, with the values of λ_1 and λ_2 ,

$$\begin{aligned} & [(n-1)b + 2\lambda_1c](na + \lambda_2b)V - [(n-1)b + 2\lambda_2c](na + \lambda_1b)U \\ &= \left[2nac - (n-1)b^2 \left[\frac{(n-2)b}{2c}(U-V) + \frac{\sqrt{n(n-2)(4ac-b^2)}}{2c}(U+V) \right] \right]. \end{aligned}$$

Then from (1),

$$\begin{aligned} \text{ord}_p(\alpha_1V - \alpha_2U) &= \text{ord}_p[(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] \\ &+ \text{ord}_p\left[\frac{2nac - (n-1)b^2}{2c}\right] - \text{ord}_p 2(na + \lambda_1b) - \text{ord}_p 2(na + \lambda_2b) \end{aligned}$$

Since $p > n$ and $\text{ord}_p b^2 > \text{ord}_p ac$, we have

$$\begin{aligned} & \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] \\ &+ \text{ord}_p ac - \text{ord}_p c - 2\text{ord}_p a \end{aligned}$$

Hence,

$$\text{ord}_p(\alpha_1V - \alpha_2U) = \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] - \text{ord}_p a$$

as asserted.

In the following theorem, we give the p-adic sizes of the variables x, y in U, V by using the assertions in Lemma 2.1 and Lemma 2.2

Theorem 2.2

Suppose U, V in $\Omega_p \times \Omega_p$ with $U = x^{\frac{n-1}{2}} + \alpha_1 x^{\frac{n-3}{2}} y$ and $V = x^{\frac{n-1}{2}} + \alpha_2 x^{\frac{n-3}{2}} y$, where

n is odd. Let $p > n$ be a prime, a, b and c in Z_p and $\text{ord}_p b^2 > \text{ord}_p ac$.

If $\text{ord}_p (n-2)b(U-V) > \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V)$, then $\text{ord}_p x \geq \frac{2}{n-1}W$ and

$$\text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right] \text{ with } W = \text{ord}_p U = \text{ord}_p V$$

Proof

From $U = x^{\frac{n-1}{2}} + \alpha_1 x^{\frac{n-3}{2}} y$ and $V = x^{\frac{n-1}{2}} + \alpha_2 x^{\frac{n-3}{2}} y$, we have

$$x = \left(\frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2} \right)^{\frac{2}{n-1}} \quad \text{and} \quad y = \frac{U - V}{(\alpha_1 - \alpha_2) x^{\frac{n-3}{2}}}$$

Then,

$$\text{ord}_p x = \frac{2}{n-1} \text{ord}_p (\alpha_1 V - \alpha_2 U) - \frac{2}{n-1} \text{ord}_p (\alpha_1 - \alpha_2) \quad (1)$$

$$\text{and } \text{ord}_p y = \text{ord}_p (U - V) - \text{ord}_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} \text{ord}_p x \quad (2)$$

From (1), Lemma 2.1 and Lemma 2.2, we obtain

$$\begin{aligned} \text{ord}_p x &= \frac{2}{n-1} \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] \\ &\quad - \frac{2}{n-1} \text{ord}_p a - \frac{2}{n-1} \left(\frac{1}{2} \text{ord}_p \frac{c}{a} \right) \end{aligned}$$

Now, from hypothesis

$$\begin{aligned} &\min \{ \text{ord}_p (n-2)b(U-V), \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V) \} \\ &= \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V) \end{aligned}$$

Hence,

$$\text{ord}_p x = \frac{2}{n-1} \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V) - \frac{1}{n-1} \text{ord}_p ac$$

Since $\text{ord}_p b^2 > \text{ord}_p ac$ and $p > n$, we have

$$\text{ord}_p x = \frac{2}{n-1} \text{ord}_p (U+V) + \frac{1}{n-1} (\text{ord}_p ac - \text{ord}_p ac)$$

That is,

$$\text{ord}_p x = \frac{2}{n-1} \text{ord}_p (U+V) \quad (3)$$

Let $W = \text{ord}_p U = \text{ord}_p V$, we have

$$\text{ord}_p x \geq \frac{2}{n-1} W$$

From (3),

$$\text{ord}_p x^{\frac{n-1}{2}} = \text{ord}_p (U+V)$$

$$\text{But } \text{ord}_p(U+V) = \text{ord}_p \left(2x^{\frac{n-1}{2}} + (\alpha_1 + \alpha_2)x^{\frac{n-3}{2}}y \right).$$

Therefore,

$$\text{ord}_p x \leq \text{ord}_p (\alpha_1 + \alpha_2)y.$$

Thus, from equation (2), Lemma 2.1 and Lemma 2.2, we have

$$\frac{n-1}{2} \text{ord}_p y \geq \text{ord}_p(U-V) - \frac{1}{2} \text{ord}_p \frac{c}{a} - \left(\frac{n-3}{2} \right) \text{ord}_p \frac{b}{a}.$$

Let $W = \text{ord}_p U = \text{ord}_p V$, we have

$$\begin{aligned} \text{ord}_p y &\geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{c}{a} + \left(\frac{n-3}{2} \right) \text{ord}_p \frac{a}{b} \right] \\ &= \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right] \end{aligned} \tag{4}$$

Therefore,

$$\text{ord}_p x \geq \frac{2}{n-1} W \text{ and } \text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right]$$

where $W = \text{ord}_p U = \text{ord}_p V$ as asserted.

Theorem 2.3 gives an estimate of the same variables in U, V under a different condition as given by the following lemma.

Lemma 2.3

Let $n > 0$ and p be an odd prime, $p > n$ and a, b, c in \mathbb{Z}_p with $\text{ord}_p b^2 > \text{ord}_p ac$. If U, V in $\Omega_p \times \Omega_p$ such that

$$\text{ord}_p (n-2)b(U-V) \leq \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V), \text{ then } \text{ord}_p V = \text{ord}_p U$$

and there exists q, w in \mathbb{Z}_p such that

$$\text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] = \beta + \text{ord}_p [(n-2)bq + \sqrt{n(n-2)(4ac-b^2)}w]$$

where $\beta = \text{ord}_p V = \text{ord}_p U$ and $\text{ord}_p q = 0$ $\text{ord}_p w \geq \text{ord}_p b - \frac{1}{2} \text{ord}_p c$, .

Proof

From $\text{ord}_p (n-2)b(U-V) \leq \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V)$, $p > n$ and

$\text{ord}_p b^2 > \text{ord}_p ac$ we obtain

$$\text{ord}_p b + \text{ord}_p (U - V) \leq \frac{1}{2} \text{ord}_p ac + \text{ord}_p (U + V)$$

Since $\text{ord}_p b^2 > \text{ord}_p ac$, this inequality becomes

$$0 < \text{ord}_p b - \frac{1}{2} \text{ord}_p ac \leq \text{ord}_p (U + V) - \text{ord}_p (U - V)$$

Therefore,

$$\text{ord}_p (U + V) > \text{ord}_p (U - V). \quad (1)$$

Now, $\text{ord}_p (U + V) - \text{ord}_p (U - V) > 0$ implies that $\text{ord}_p U = \text{ord}_p V$. This is because if,

$\text{ord}_p U \neq \text{ord}_p V$ we have $\text{ord}_p (U + V) - \text{ord}_p (U - V) = 0$.

Suppose $\beta = \text{ord}_p U = \text{ord}_p V$.

Then,

$$U = p^\beta k \text{ and } V = p^\beta l \text{ with } \text{ord}_p k = 0 \text{ and } \text{ord}_p l = 0.$$

Thus,

$$U + V = p^\beta(k+l) \text{ and } U - V = p^\beta(k-l).$$

From (1), we obtain

$$\text{ord}_p (k+l) > \text{ord}_p (k-l).$$

This means that, $\text{ord}_p [(k+l) + (k-l)] = \text{ord}_p (k-l)$

That is,

$$\text{ord}_p k = \text{ord}_p (k-l) = 0$$

Therefore,

$$\text{ord}_p (k+l) > 0$$

Suppose $q = k-l$ and $w = k+l$.

$$\begin{aligned} \text{ord}_p (U + V) - \text{ord}_p (U - V) &= \beta + \text{ord}_p (k+l) - \beta - \text{ord}_p (k-l) \\ &= \text{ord}_p (k+l) = \text{ord}_p w \end{aligned}$$

But $\text{ord}_p (U + V) - \text{ord}_p (U - V) \geq \text{ord}_p b - \frac{1}{2} \text{ord}_p ac$.

Then,

$$\text{ord}_p w \geq \text{ord}_p b - \frac{1}{2} \text{ord}_p ac.$$

Hence,

$$\begin{aligned} & \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] \\ &= \text{ord}_p [(n-2)bp^\beta q + \sqrt{n(n-2)(4ac-b^2)}p^\beta w] \end{aligned}$$

with $\text{ord}_p q=0$ and $\text{ord}_p w \geq \text{ord}_p b - \frac{1}{2}\text{ord}_p c$.

The right expression becomes

$$\begin{aligned} & \text{ord}_p p^\beta [(n-2)bq + \sqrt{n(n-2)(4ac-b^2)}w] \\ &= \beta + \text{ord}_p [(n-2)bq + \sqrt{n(n-2)(ac-b^2)}w] \end{aligned}$$

with $\beta = \text{ord}_p U = \text{ord}_p V$, $\text{ord}_p q=0$ and $\text{ord}_p w \geq \text{ord}_p b - \frac{1}{2}\text{ord}_p ac$

as asserted.

Theorem 2.3

Suppose U, V in $\Omega_p \times \Omega_p$ with $U = x^{\frac{n-1}{2}} + \alpha_1 x^{\frac{n-3}{2}} y$ and $V = x^{\frac{n-1}{2}} + \alpha_2 x^{\frac{n-3}{2}} y$ where n is odd. Let $p > n$ be a prime, a, b and c in Z_p and $\text{ord}_p b^2 > \text{ord}_p ac$.

If $\text{ord}_p (n-2)b(U-V) \leq \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V)$ then $\text{ord}_p x \geq \frac{2}{n-1}\text{ord}_p W$

and $\text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2}\text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right]$ with $W = \text{ord}_p V = \text{ord}_p U$.

Proof

Suppose $x = \left(\frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2} \right)^{\frac{2}{n-1}}$ and $y = \frac{U-V}{(\alpha_1 - \alpha_2)x^{\frac{n-3}{2}}}$.

Then,

$$\text{ord}_p x = \frac{2}{n-1}\text{ord}_p (\alpha_1 V - \alpha_2 U) - \frac{2}{n-1}\text{ord}_p (\alpha_1 - \alpha_2) \tag{1}$$

$$\text{and } \text{ord}_p y = \text{ord}_p (U - V) - \text{ord}_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} \text{ord}_p x \quad (2)$$

From (1) and by Lemma 2.1 and Lemma 2.2, we have

$$\begin{aligned} \text{ord}_p x &= \frac{2}{n-1} \text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] \\ &\quad - \frac{2}{n-1} \text{ord}_p a - \frac{2}{n-1} \left(\frac{1}{2} \text{ord}_p \frac{c}{a} \right) \end{aligned}$$

By Lemma 2.3, there exists q and w in Z_p such that

$$\text{ord}_p x = \frac{2}{n-1} \left(\beta + \text{ord}_p [(n-2)bq + \sqrt{n(n-2)(4ac-b^2)}w] \right) - \frac{1}{n-1} \text{ord}_p ac$$

with $\beta = \text{ord}_p V = \text{ord}_p U$, $\text{ord}_p q = 0$, and $\text{ord}_p w > 0$.

Suppose $W = \beta$, we find that

$$\text{ord}_p x \geq \frac{2}{n-1} \left(W + \min \left\{ \text{ord}_p b, \frac{1}{2} \text{ord}_p ac + \text{ord}_p w \right\} \right) - \frac{1}{n-1} \text{ord}_p ac$$

Then,

$$\text{ord}_p x \geq \frac{2}{n-1} W$$

From (1) and (2), we have

$$\begin{aligned} \text{ord}_p y &= \text{ord}_p (U - V) - \text{ord}_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} \text{ord}_p x \\ &= \text{ord}_p (U - V) - \text{ord}_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} \left[\frac{2}{n-1} \text{ord}_p (\alpha_1 V - \alpha_2 U) - \frac{2}{n-1} \text{ord}_p (\alpha_1 - \alpha_2) \right] \end{aligned}$$

By Lemma 2.2, we have

$$\begin{aligned} \text{ord}_p y &= \text{ord}_p (U - V) - \frac{2}{(n-1)} \text{ord}_p (\alpha_1 - \alpha_2) \\ &\quad - \frac{(n-3)}{(n-1)} \left[\text{ord}_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)] - \text{ord}_p a \right] \end{aligned}$$

Since $p > n$ and $\text{ord}_p (n-2)b(U-V) \leq \text{ord}_p \sqrt{n(n-2)(4ac-b^2)}(U+V)$, we have

$$\text{ord}_p y = \text{ord}_p (U-V) - \frac{2}{(n-1)} \text{ord}_p (\alpha_1 - \alpha_2) - \frac{(n-3)}{(n-1)} [\text{ord}_p b(U-V) - \text{ord}_p a]$$

By Lemma 2.1, we have

$$\begin{aligned} \text{ord}_p y &= \frac{2}{n-1} \text{ord}_p (U-V) - \frac{2}{(n-1)} \left[\frac{1}{2} \text{ord}_p \frac{c}{a} \right] - \frac{(n-3)}{(n-1)} [\text{ord}_p b - \text{ord}_p a] \\ &= \frac{2}{n-1} \left[\text{ord}_p (U-V) - \frac{1}{2} \text{ord}_p \frac{c}{a} - \frac{(n-3)}{2} \text{ord}_p b + \frac{(n-3)}{2} \text{ord}_p a \right] \\ &= \frac{2}{n-1} \left[\text{ord}_p (U-V) - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right] \end{aligned}$$

Let $W = \text{ord}_p V = \text{ord}_p U$,

$$\text{we have } \text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right].$$

Therefore,

$$\text{ord}_p x \geq \frac{2}{n-1} \text{ord}_p V \text{ and } \text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right]$$

with $W = \text{ord}_p U = \text{ord}_p V$ as asserted.

The following theorem gives explicit estimates of the x, y variables in U and V in terms of p -adic sizes of integers in Z_p . The proof utilizes the result obtained above.

Theorem 2.4

Suppose U, V in $\Omega_p \times \Omega_p$ with $U = x^{\frac{n-1}{2}} + \alpha_1 x^{\frac{n-3}{2}} y$ and $V = x^{\frac{n-1}{2}} + \alpha_2 x^{\frac{n-3}{2}} y$ where

n is odd. Let $p > n$ be a prime, a, b, c, s and t in Z_p , $\text{ord}_p b^2 > \text{ord}_p ac$, $\delta = \max\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p c\}$ and $\text{ord}_p s, \text{ord}_p t \geq \alpha > \delta$.

If $\text{ord}_p U = \frac{1}{2} \text{ord}_p \frac{s + \lambda_1 t}{na + \lambda_1 b}$ and $\text{ord}_p V = \frac{1}{2} \text{ord}_p \frac{s + \lambda_2 t}{na + \lambda_2 b}$ then $\text{ord}_p x \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$ and

$$\text{ord}_p y \geq \frac{1}{n-1} (\alpha - (n-3)\delta).$$

Proof

From $U = x^{\frac{n-1}{2}} + \alpha_1 x^{\frac{n-3}{2}} y$ and $V = x^{\frac{n-1}{2}} + \alpha_2 x^{\frac{n-3}{2}} y$, we have

$$x = \left(\frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2} \right)^{\frac{2}{n-1}} \text{ and } y = \frac{U - V}{(\alpha_1 - \alpha_2) x^{\frac{n-3}{2}}}.$$

Then,

$$\text{ord}_p x = \frac{2}{n-1} \text{ord}_p (\alpha_1 V - \alpha_2 U) - \frac{2}{n-1} \text{ord}_p (\alpha_1 - \alpha_2) \text{ and}$$

$$\text{ord}_p y = \text{ord}_p (U - V) - \text{ord}_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} \text{ord}_p x$$

From Theorems 2.2 and 2.3, we obtain that

$$\text{ord}_p x \geq \frac{2}{n-1} W \tag{1}$$

$$\text{and } \text{ord}_p y \geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right] \tag{2}$$

with $W = \text{ord}_p U = \text{ord}_p V$ and $\text{ord}_p U = \frac{1}{2} \text{ord}_p \frac{s + \lambda_1 t}{na + \lambda_1 b}$, $\text{ord}_p V = \frac{1}{2} \text{ord}_p \frac{s + \lambda_2 t}{na + \lambda_2 b}$.

From (1),

$$\text{we have } \text{ord}_p x \geq \frac{1}{n-1} \text{ord}_p \left(\frac{s + \lambda_i t}{na + \lambda_i b} \right), i=1,2.$$

By proof of Lemma 2.1, $\text{ord}_p 2(na + \lambda_i b) = \text{ord}_p a$ for $i=1,2$.

$$\text{Then, } \text{ord}_p x \geq \frac{1}{n-1} [\text{ord}_p (s + \lambda_i t) - \text{ord}_p a], i=1,2. \tag{3}$$

Suppose $\min\{\text{ord}_p s, \text{ord}_p \lambda_i t\} = \text{ord}_p s$, $i=1,2$ we have $\text{ord}_p x \geq \frac{1}{n-1} (\text{ord}_p s - \text{ord}_p a)$

Then, by hypothesis,

$$\text{ord}_p x \geq \frac{1}{n-1} (\alpha - \delta)$$

Now from (2),

$$\begin{aligned} \text{ord}_p y &\geq \frac{2}{n-1} \left[W - \frac{1}{2} \text{ord}_p \frac{cb^{(n-3)}}{a^{(n-2)}} \right] \\ &= \frac{2}{n-1} \left[\frac{1}{2} \text{ord}_p \frac{s + \lambda_2 t}{na + \lambda_2 b} - \frac{1}{2} \text{ord}_p \frac{c}{a} + \binom{n-3}{2} \text{ord}_p \frac{a}{b} \right] \\ &\geq \frac{1}{n-1} \text{ord}_p \left(\frac{s + \lambda_2 t}{na + \lambda_2 b} \right) - \binom{n-3}{n-1} \left[\text{ord}_p \frac{b}{a} + \text{ord}_p c \right] \end{aligned}$$

By the proof of Lemma 2.1, $\text{ord}_p 2(na + \lambda_i b) = \text{ord}_p a$ for $i=1,2$. Then

$$\begin{aligned} \text{ord}_p y &\geq \frac{1}{n-1} \text{ord}_p (s + \lambda_i t) - \frac{1}{n-1} \text{ord}_p a + \binom{n-3}{n-1} \text{ord}_p a, \\ &\quad - \binom{n-3}{n-1} \max\{\text{ord}_p b, \text{ord}_p c\} \\ &\geq \frac{1}{n-1} \left[\text{ord}_p (s + \lambda_i t) - (n-3) \max\{\text{ord}_p b, \text{ord}_p c\} \right], \quad i=1,2. \end{aligned}$$

By the same method for $\text{ord}_p x$ from equation (3), we have

$$\text{ord}_p y \geq \frac{1}{n-1} (\alpha - (n-3)\delta).$$

We will get the same result if $\min\{\text{ord}_p s, \text{ord}_p \lambda_2 t\} = \text{ord}_p \lambda_i t$ because

$$\text{ord}_p a < \text{ord}_p \lambda_i b, \quad i=1,2.$$

Therefore,

$$\text{ord}_p x \geq \frac{1}{n-1} (\alpha - \delta) \geq \frac{1}{n-1} \text{ord}_p (\alpha - (n-3)\delta) \quad \text{and} \quad \text{ord}_p y \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$$

as asserted.

Theorem 2.5

Let $f(x,y) = ax^n + bx^{n-1}y + cx^{n-2}y^2 + sx + ty + k$ be a polynomial in $Z_p[x, y]$ with $p > n$ and n is odd. Let $\alpha > 0$, $\delta = \max\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p c\}$ and $\text{ord}_p b^2 > \text{ord}_p ac$.

If $ord_p f_x(0,0), ord_p f_y(0,0) \geq \alpha > \delta$ there exist (ξ, η) such that $f_x(\xi, \eta) = 0, f_y(\xi, \eta) = 0$ and $ord_p \xi \geq \frac{1}{n-1}(\alpha - (n-3)\delta), ord_p \eta \geq \frac{1}{n-1}(\alpha - (n-3)\delta)$.

Proof

Let $g = f_x$ and $h = f_y$ and λ be a constant. Then,

$$(g + \lambda h)(x, y) = (na + \lambda b)x^{n-1} + ((n-1)b + 2\lambda c)x^{n-2}y + (n-2)cx^{n-3}y^2 + s + \lambda t$$

and

$$\frac{(g + \lambda h)(x, y)}{na + \lambda b} = x^{n-1} + \left(\frac{(n-1)b + 2\lambda c}{na + \lambda b}\right)x^{n-2}y + \left(\frac{(n-2)c}{na + \lambda b}\right)x^{n-3}y^2 + \frac{s + \lambda t}{na + \lambda b} \tag{1}$$

By completing the square in equation (1), we have

$$\frac{(g + \lambda h)(x, y)}{na + \lambda b} = \left(x^{\frac{n-1}{2}} + \frac{(n-1)b + 2\lambda c}{2(na + \lambda b)}x^{\frac{n-3}{2}}y\right)^2 + \frac{s + \lambda t}{na + \lambda b} \tag{2}$$

if $\frac{(n-2)c}{na + \lambda b} - \left(\frac{(n-1)b + 2\lambda c}{2(na + \lambda b)}\right)^2 = 0$.

That is, $4c^2\lambda^2 + 4bc\lambda + (n-1)^2b^2 - 4n(n-2)ac = 0$. (3)

From (3), we will get two values of λ , say λ_1, λ_2 , where

$$\lambda_1 = \frac{-b + \sqrt{n(n-2)(4ac - b^2)}}{2c} \text{ and } \lambda_2 = \frac{-b - \sqrt{n(n-2)(4ac - b^2)}}{2c}$$

$\lambda_1 \neq \lambda_2$, because $ord_p b^2 > ord_p ac$ of means that $b^2 \neq ac$.

Now, let

$$U = x^{\frac{n-1}{2}} + \frac{(n-1)b + 2\lambda_1 c}{2(na + \lambda_1 b)}x^{\frac{n-3}{2}}y, \tag{4}$$

$$V = x^{\frac{n-1}{2}} + \frac{(n-1)b + 2\lambda_2 c}{2(na + \lambda_2 b)}x^{\frac{n-3}{2}}y, \tag{5}$$

$$F(U, V) = (g + \lambda_1 h)(x, y) \tag{6}$$

and $G(U, V) = (g + \lambda_2 h)(x, y)$. (7)

By substitution of U and V in (2), we obtain the following polynomials in (U, V)

$$F(U, V) = (na + \lambda_1 b)U^2 + s + \lambda_1 t \quad (8)$$

$$G(U, V) = (na + \lambda_2 b)V^2 + s + \lambda_2 t \quad (9)$$

The combination of the indicator diagrams associated with the Newton polyhedron of (8) and (9) takes the form shown in Figure 1.

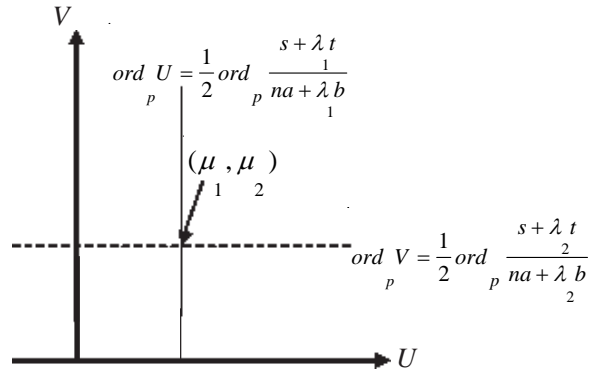


Figure 1: The indicator diagrams of $F(U, V) = (na + \lambda_1 b)U^2 + s + \lambda_1 t$ and $G(U, V) = (na + \lambda_2 b)V^2 + s + \lambda_2 t$

From Figure 1 and Theorem 2.1 there exists (\hat{U}, \hat{V}) in $\Omega_p \times \Omega_p$ such that $F(\hat{U}, \hat{V}) = 0$,

$$G(\hat{U}, \hat{V}) = 0 \text{ and } \text{ord}_p \hat{U} = \mu_1, \text{ ord}_p \hat{V} = \mu_2 \text{ where } \mu_1 = \frac{1}{2} \text{ord}_p \frac{s + \lambda_1 t}{na + \lambda_1 b} \text{ and}$$

$$\mu_2 = \frac{1}{2} \text{ord}_p \frac{s + \lambda_2 t}{na + \lambda_2 b}$$

Suppose $U = \hat{U}$ and $V = \hat{V}$ in (4) and (5). There exists (x_0, y_0) such that

$$x_0 = \left(\frac{\alpha_1 \hat{V} - \alpha_2 \hat{U}}{\alpha_1 - \alpha_2} \right)^{\frac{2}{n-1}} \text{ and } y_0 = \frac{\hat{U} - \hat{V}}{(\alpha_1 - \alpha_2) x_0^{\frac{n-3}{2}}}$$

with $\alpha_1 = \frac{(n-1)b + 2\lambda_1 c}{2(na + \lambda_1 b)}$, $\alpha_2 = \frac{(n-1)b + 2\lambda_2 c}{2(na + \lambda_2 b)}$ in which λ_1, λ_2 are the zeros of

$$h(\lambda) = 4c^2\lambda^2 + 4bc\lambda + (n-1)^2b^2 - 4n(n-2)ac \text{ and } \alpha_1 \neq \alpha_2 \text{ because of } \lambda_1 \neq \lambda_2$$

From Theorem 2.4, we have

$$\text{ord}_p x_0 \geq \frac{1}{n-1} \text{ord}_p (\alpha - (n-3)\delta) \text{ and } \text{ord}_p y_0 \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$$

Let $\xi = x_0$ and $\eta = y_0$

Now, we show that $g(\xi, \eta) = f_x(\xi, \eta) = 0$ and $h(\xi, \eta) = f_y(\xi, \eta) = 0$.

From (6) and (7), we obtain $F(\hat{U}, \hat{V}) = (g + \lambda_1 h)(\xi, \eta)$ and $G(\hat{U}, \hat{V}) = (g + \lambda_2 h)(\xi, \eta)$.

$$\text{Because of } F(\hat{U}, \hat{V}) = 0, \text{ then } g(\xi, \eta) + \lambda_1 h(\xi, \eta) = 0 \tag{10}$$

$$\text{Also } G(\hat{U}, \hat{V}) = 0. \text{ Therefore } g(\xi, \eta) + \lambda_2 h(\xi, \eta) = 0 \tag{11}$$

Since $\lambda_1 \neq \lambda_2$ and from (10) and (11), $(\lambda_1 - \lambda_2)h(\xi, \eta) = 0$, we obtain $h(\xi, \eta) = 0$.

Similarly $g(\xi, \eta) = 0$.

Then, $\text{ord}_p \xi \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$ and $\text{ord}_p \eta \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$ where (ξ, η) are the zeros of g and h and $\delta = \max\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p c\}$.

We will get a sharper result if $\text{ord}_p a > \text{ord}_p b$, as written in the following theorem:

Theorem 2.6

Let $f(x, y) = ax^n + bx^{n-1}y + cx^{n-2}y^2 + sx + ty + k$ be a polynomial in $Z_p[x, y]$ where $p > n$ and n is odd. Let $\alpha > 0$, $\delta = \max\{\text{ord}_p a, \text{ord}_p c\}$, $\text{ord}_p b^2 > \text{ord}_p ac$ and $\text{ord}_p a > \text{ord}_p b$.

If $\text{ord}_p f_x(0, 0), \text{ord}_p f_y(0, 0) \geq \alpha > \delta$ there exists (ξ, η) such that $f_x(\xi, \eta) = 0, f_y(\xi, \eta) = 0$ and

$$\text{ord}_p \xi \geq \frac{1}{n-1} (\alpha - \delta), \text{ ord}_p \eta \geq \frac{1}{n-1} (\alpha - \delta)$$

Proof

By proof of Theorems 2.4 and 2.5, there exists x_0 and y_0 such that

$$\text{ord}_p x_0 \geq \frac{1}{n-1} (\alpha - \delta),$$

$$\text{ord}_p y_0 \geq \frac{2}{n-1} \left[\frac{1}{2} \text{ord}_p \frac{s + \lambda_1 t}{na + \lambda_1 b} - \frac{1}{2} \text{ord}_p \frac{c}{a} + \left(\frac{n-3}{2} \right) \text{ord}_p \frac{a}{b} \right] \text{ i } = 1, 2.$$

By proof of Lemma 2.1, $ord_p 2(na + \lambda_i b) = ord_p a$ for $i = 1, 2$. Then

$$ord_p y_0 \geq \frac{2}{n-1} \left[\frac{1}{2} ord_p (s + \lambda_i t) - \frac{1}{2} ord_p a + \frac{1}{2} ord_p \frac{c}{a} - \left(\frac{n-3}{2} \right) ord_p \frac{b}{a} \right]$$

That is,

$$ord_p y_0 \geq \frac{2}{n-1} \left[\frac{1}{2} ord_p (s + \lambda_i t) - \frac{1}{2} ord_p c + \left(\frac{n-3}{2} \right) ord_p \frac{a}{b} \right]$$

where $i = 1, 2$.

By the hypothesis $ord_p a > ord_p b$, we have

$$ord_p y_0 \geq \frac{2}{n-1} \left[\frac{1}{2} ord_p (s + \lambda_i t) - \frac{1}{2} ord_p c \right], i = 1, 2$$

Similarly, by the same method for $ord_p x$ from equation (3) in Theorem 2.4, we have

$$ord_p y_0 \geq \frac{1}{n-1} (\alpha - \delta)$$

Suppose $\xi = x_0$ and $\eta = y_0$.

Hence,

$$ord_p \xi \geq \frac{1}{n-1} (\alpha - \delta) \quad \text{and} \quad ord_p \eta \geq \frac{1}{n-1} (\alpha - \delta)$$

where $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ as asserted.

CONCLUSION

Our investigation shows that if p is an odd prime $p > n$,

$f(x, y) = ax^n + bx^{n-1}y + cx^{n-2}y^2 + sx + ty + k$ a polynomial in $Z_p[x, y]$ where n is odd,

$\alpha > \delta$, $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ and $ord_p b^2 > ord_p ac$ then the p -adic sizes of the

common zeros (ξ, η) of the partial derivatives of this polynomial is

$ord_p \xi \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$, $ord_p \eta \geq \frac{1}{n-1} (\alpha - (n-3)\delta)$. We obtain a sharper result if

$ord_p a > ord_p b$, that is $ord_p \xi \geq \frac{1}{n-1} (\alpha - \delta)$, $ord_p \eta \geq \frac{1}{n-1} (\alpha - \delta)$ with

$\delta = \max\{ord_p a, ord_p c\}$.

REFERENCES

- CHAN, K.L. and K.A. MOHD. ATAN. 1997. On the estimate to solutions of congruence equations associated with a quartic form. *Journal of Physical Science* **8**: 21-34.
- HENG, S.H. and K.A. MOHD ATAN. 1999. An estimation of exponential sums associated with a cubic form. *Journal of Physical Science* **10**: 1-21.
- KOBLITZ, N. 1977. *p -adic Numbers, p -adic analysis and zeta Function*. New York: Springer-Verlag.
- LOXTON, J.H. and R.C. VAUGHN. 1985. The estimate of complete exponential sums. *Canad. Mth Bull.* **28(4)**: 440-454 .
- MOHD. ATAN, K.A. 1986. Newton polyhedral method of determining p -adic orders of zeros common to two polynomials in. *Pertanika* **9(3)**: 375-380. Universiti Pertanian Malaysia.
- MOHD. ATAN, K.A. and I.B. ABDULLAH. 1992. Set of solution to congruences equations associated with cubic form. *Journal of Physical Science* **3**: 1-6.
- MOHD. ATAN, K.A. and J.H. LOXTON. 1986. Newton polyhedral and solutions of congruences. In *Diophantine Analysis*, ed. J.H. Loxton and A. Van der Poorten. Cambridge: Cambridge University Press.
- SAPAR, S.H. and K.A. MOHD ATAN. 2002. Estimate for the cardinality of the set of solution to congruence equations. *Journal of Technology* No. 36(C) (Malay): 13-40.