Malaysian Journal of Mathematical Sciences **1(1)**: 23 - 43 (2007)

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

[1] **Sapar S.H. & [2]Mohd Atan K.A.**
[1]*Mathematics Department, Faculty of Science*
[2]*Laboratory of Theoretical Mathematics, Institute for Mathematical Research,*
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
E-mail: [1]sitihas@fsas.upm.edu.my ; [2]kamel@putra.upm.edu.my

ABSTRACT

Let $\underline{x} = (x_1, x_2, \ldots, x_n)$ 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 Q_p the field of rational p-adic numbers and the highest power of p, which divides x. For each prime p, let $\underline{f} = (f_1, f_2, \ldots, f_n)$ be an n-tuple polynomials in $Z_p[\underline{x}]$, where Z_p is the ring of p-adic integers and $\underline{x} = (x_1, x_2, \ldots, x_n)$.

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 $S(f;q) = \sum_{\underline{x} \bmod q} \exp\left(\frac{2\pi i f}{q}\right)$ where $f(\underline{x})$ is a polynomial in $Z[\underline{x}]$ 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 $f(x,y) = ax^3 + bx^2y + cx + dy + e$. He found that the p-adic sizes for the zero (ξ,η) of this polynomial is $ord_p \xi \geq \frac{1}{2}(\alpha - \delta)$ and $ord_p \eta \geq \frac{1}{2}(\alpha - \delta)$ with $\delta = \max\left\{ord_p 3a, \frac{3}{2} ord_p b\right\}$.

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

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 polynomialis $ord_p \xi \geq \frac{1}{3}(\alpha - \delta)$ and $ord_p \eta \geq \frac{1}{3}(\alpha - \delta)$ with

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

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

$$\alpha_1 = \frac{(n-1)b + 2\lambda_1 c}{2(na + \lambda_1 b)} \text{ and } \alpha_2 = \frac{(n-1)b + 2\lambda_2 c}{2(na + \lambda_2 b)}$$

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

Proof:

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

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

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

.

Since $ord_p b^2 > ord_p ac$ and $p > n$, we have

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

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

Thus , $ord_p 2\lambda_1 c = \frac{1}{2} ord_p ac < ord_p b.$

By the same method, it can be shown that

$$ord_p 2\lambda_2 c = \frac{1}{2} ord_p ac < ord_p b .$$

Therefore,

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

Consider that

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

Then,

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

.

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

$$ord_p \lambda_1 b = ord_p b + \frac{1}{2} ord_p ac - ord_p c$$

$$> \frac{1}{2} ord_p ac + \frac{1}{2} ord_p ac - ord_p c$$

$$= ord_p a.$$

Thus, $ord_p \lambda_1 b > ord_p a$

Again by the same method, we can show that

$$ord_p \lambda_2 b > ord_p a$$

Therefore, we obtain that

$$ord_p 2(na+\lambda_i b) = ord_p a, i=1,2 \tag{2}$$

From (1) and (2),

$$ord_p \alpha_i = ord_p\left(\frac{(n-1)b+2\lambda_i c}{2(na+\lambda_i b)}\right), i = 1,2$$

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

.

That is, $ord_p \alpha_i = \frac{1}{2} ord_p \frac{c}{a}, i = 1,2$ (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 $\lambda_1 - \lambda_2 = \dfrac{\sqrt{n(n-2)(4ac-b^2)}}{c}$

Then,

$$ord_p(\alpha_1 - \alpha_2) = ord_p\sqrt{n(n-2)(4ac-b^2)} - ord_p c + ord_p(2nac-(n-1)b^2)$$
$$-ord_p 2(na+\lambda_1 b) - ord_p(na+\lambda_2 b)$$

Since $p>n$, $ord_p b^2 > ord_p ac$ and from (2), we have

$$ord_p(\alpha_1 - \alpha_2) = \frac{1}{2}ord_p ac - ord_p c + ord_p ac - 2ord_p a$$
$$= \frac{1}{2}\left(ord_p c - ord_p a\right)$$

That is, $ord_p(\alpha_1 - \alpha_2) = \dfrac{1}{2}\left(ord_p \dfrac{c}{a}\right)$ (4)

From (3) and (4), we obtain

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

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

Then

$$ord_p(\alpha_1 + \alpha_2) = ord_p \frac{2b}{c}((2-n)(1+n)b^2 + 6n(n-2)ac)$$
$$-ord_p 2(na+\lambda_1 b) - ord_p(na+\lambda_2 b)$$

Since $p>n$, $ord_p b^2 > ord_p ac$ and from (2), we have

$$ord_p(\alpha_1+\alpha_2) = ord_p \frac{b}{c} + ord_p ac - 2ord_p a$$

$$= ord_p \frac{b}{a}$$

Therefore, we obtain

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

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

In the Lemma 2.2 and Theorem 2.2,

$\alpha_1 = \frac{(n-1)b + 2\lambda_1 c}{2(na+\lambda_1 b)}$, $\alpha_2 = \frac{(n-1)b+2\lambda_2 c}{2(na+\lambda_2 b)}$ where λ_1, λ_2 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 Ω_p x Ω_p. Let $n>1$ be a positive integer and $p>n$ be a prime, a, b and c in Z_p.

If $ord_p b^2 > ord_p ac$, then

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

Proof

$$ord_p(\alpha_1 V - \alpha_2 U) = ord_p\left(\frac{(n-1)b+2\lambda_1 c}{2(na+\lambda_1 b)}V - \frac{(n-1)b+2\lambda_2 c}{2(na+\lambda_2 b)}U\right)$$

$$= ord_p\left[[(n-1)b+2\lambda_1 c](na+\lambda_2 b)V - [(n-1)b+2\lambda_2 c](na+\lambda_1 b)U\right]$$

$$- ord_p 2(na+\lambda_1 b) - ord_p 2(na+\lambda_2 b) \qquad (1)$$

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

$$[(n-1)b + 2\lambda_1 c](na + \lambda_2 b)V - [(n-1)b + 2\lambda_2 c](na + \lambda_1 b)U$$

$$= \left[2nac - (n-1)b^2\right]\left[\frac{(n-2)b}{2c}(U - V) + \frac{\sqrt{n(n-2)(4ac - b^2)}}{2c}(U + V)\right].$$

Then from (1),

$$ord_p(\alpha_1 V - \alpha_2 U) = ord_p[(n-2)b(U - V) + \sqrt{n(n-2)(4ac - b^2)}(U + V)]$$

$$+ ord_p\left[\frac{2nac - (n-1)b^2}{2c}\right] - ord_p 2(na + \lambda_1 b) - ord_p 2(na + \lambda_2 b)$$

Since $p > n$ and $ord_p b^2 > ord_p ac$, we have

$$ord_p[(n-2)b(U - V) + \sqrt{n(n-2)(4ac - b^2)}(U + V)]$$

$$+ ord_p ac - ord_p c - 2ord_p a$$

Hence,

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

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 $ord_p b^2 > ord_p ac$.

If $ord_p (n-2)b(U - V) > ord_p \sqrt{n(n-2)(4ac - b^2)}(U + V)$, then $ord_p x \geq \frac{2}{n-1}W$ and $ord_p y \geq \frac{2}{n-1}\left[W - \frac{1}{2} ord_p \frac{cb^{(n-3)}}{a^{(n-2)}}\right]$ with $W = ord_p U = ord_p V$.

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

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

Then,

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

and $$ord_p y = ord_p (U - V) - ord_p (\alpha_1 - \alpha_2) - \frac{n-3}{2} ord_p x \tag{2}$$

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

$$ord_p x = \frac{2}{n-1} ord_p [(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2)}(U+V)]$$
$$- \frac{2}{n-1} ord_p a - \frac{2}{n-1} \left(\frac{1}{2} ord_p \frac{c}{a} \right)$$

Now, from hypothesis

$$\min \{ord_p (n-2)b(U-V), ord_p \sqrt{n(n-2)(4ac-b^2)}(U+V)\}$$
$$= ord_p \sqrt{n(n-2)(4ac-b^2)}(U+V) \quad .$$

Hence,

$$ord_p x = \frac{2}{n-1} ord_p \sqrt{n(n-2)(4ac-b^2)}(U+V) - \frac{1}{n-1} ord_p ac \, .$$

Since $ord_p b^2 > ord_p ac$ and $p > n$, we have

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

That is,

$$ord_p x = \frac{2}{n-1} ord_p (U+V) \tag{3}$$

Let $W = ord_p U = ord_p V$, we have

$$ord_p x \geq \frac{2}{n-1} W$$

From (3),

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

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

Therefore,

$$ord_p x \le ord_p(\alpha_1+\alpha_2)y \ .$$

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

$$\frac{n-1}{2}ord_p y \ge ord_p(U-V) - \frac{1}{2}ord_p\frac{c}{a} - \left(\frac{n-3}{2}\right)ord_p\frac{b}{a}.$$

Let $W=ord_pU = ord_pV$, we have

$$ord_p y \ge \frac{2}{n-1}\left[W - \frac{1}{2}ord_p\frac{c}{a} + \left(\frac{n-3}{2}\right)ord_p\frac{a}{b}\right] \quad (4)$$

$$= \frac{2}{n-1}\left[W - \frac{1}{2}ord_p\frac{cb^{(n-3)}}{a^{(n-2)}}\right]$$

Therefore,

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

where $W= ord_pU= ord_pV$ 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 Zp with $ord_pb^2>ord_pac$. If U,V in $\Omega_p \times \Omega_p$ such that

$$ord_p(n-2)b(U-V) \le ord_p\sqrt{n(n-2)(4ac-b^2)}(U+V)\text{, then } ord_pV=ord_pU$$

and there exists q, w in Z_p such that

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

where $\beta = ord_pV = ord_pU$ and $ord_pq = 0$ $ord_pw \ge ord_pb - \frac{1}{2}ord_pc$, .

Proof

From $ord_p(n-2)b(U-V) \le ord_p\sqrt{n(n-2)(4ac-b^2)}(U+V)$, $p>n$ and

$ord_pb^2 > ord_pac$ we obtain

$$ord_p b + ord_p (U - V) \le \frac{1}{2} ord_p ac + ord_p (U + V)$$

Since $ord_p b^2 > ord_p ac$, this inequality becomes

$$0 < ord_p b - \frac{1}{2} ord_p ac \le ord_p (U + V) - ord_p (U - V)$$

Therefore,

$$ord_p(U + V) > ord_p(U-V). \qquad (1)$$

Now, $ord_p(U + V) - ord_p(U-V) > 0$ implies that $ord_p U = ord_p V$. This is because if , $ord_p U \neq ord_p V$ we have $ord_p (U + V) - ord_p (U - V) = 0$.

Suppose $\beta = ord_p U = ord_p V$.

Then,

$U = p^\beta k$ and $V = p^\beta l$ with $ord_p k = 0$ and $ord_p l = 0$.

Thus,

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

From (1), we obtain

$$ord_p(k+l) > ord_p(k-l).$$

This means that, $ord_p [(k + l) + (k - l)] = ord_p (k - l)$

That is,

$$ord_p k = ord_p(k-l) = 0$$

Therefore,

$$ord_p(k+l) > 0$$

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

$$ord_p (U + V) - ord_p (U - V) = \beta + ord_p (k + l) - \beta - ord_p (k - l)$$

$$= ord_p (k + l) = ord_p w$$

But $ord_p (U + V) - ord_p (U - V) \ge ord_p b - \frac{1}{2} ord_p ac$.

Then ,

$$ord_p w \ge ord_p b - \frac{1}{2} ord_p ac \ .$$

Hence,

$$ord_p[(n-2)b(U-V)+\sqrt{n(n-2)(4ac-b^2)}(U+V)]$$

$$=ord_p[(n-2)bp^{\beta}q+\sqrt{n(n-2)(4ac-b^2)}\,p^{\beta}w]$$

with $ord_p\, q=0$ and $ord_p w \geq ord_p b - \frac{1}{2} ord_p c$.

The right expression becomes

$$ord_p\, p^{\beta}[(n-2)bq+\sqrt{n(n-2)(4ac-b^2)}w]$$

$$= \beta + ord_p[(n-2)bq+\sqrt{n(n-2)(ac-b^2)}w]$$

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

as asserted.

Theorem 2.3

Suppose U,V in Ω_p x Ω_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 $ord_p b^2 > ord_p ac$.

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

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

Proof

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

Then,

$$ord_p x = \frac{2}{n-1} ord_p(\alpha_1 V - \alpha_2 U) - \frac{2}{n-1} ord_p(\alpha_1 - \alpha_2) \qquad (1)$$

and $ord_p y = ord_p(U-V) - ord_p(\alpha_1 - \alpha_2) - \frac{n-3}{2} ord_p x$ (2)

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

$$ord_p x = \frac{2}{n-1} ord_p[(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2}(U+V)]$$

$$-\frac{2}{n-1} ord_p a - \frac{2}{n-1}\left(\frac{1}{2} ord_p \frac{c}{a}\right)$$

.

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

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

with $\beta = ord_p V = ord_p U$, $ord_p q = 0$, and $ord_p w > 0$.

Suppose $W = \beta$, we find that

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

Then,

$$ord_p x \geq \frac{2}{n-1} W$$

From (1) and (2), we have

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

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

By Lemma 2.2, we have

$$ord_p y = ord_p(U-V) - \frac{2}{(n-1)} ord_p(\alpha_1 - \alpha_2)$$

$$-\frac{(n-3)}{(n-1)}\left[ord_p[(n-2)b(U-V) + \sqrt{n(n-2)(4ac-b^2}(U+V)] - ord_p a\right]$$

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

$$ord_p y = ord_p\left(U-V\right) - \frac{2}{(n-1)} ord_p\left(\alpha_1-\alpha_2\right) - \frac{(n-3)}{(n-1)}\left[ord_p b(U-V) - ord_p a\right]$$

By Lemma 2.1, we have

$$ord_p y = \frac{2}{n-1} ord_p\left(U-V\right) - \frac{2}{(n-1)}\left[\frac{1}{2} ord_p \frac{c}{a}\right] - \frac{(n-3)}{(n-1)}\left[ord_p b - ord_p a\right]$$

$$= \frac{2}{n-1}\left[ord_p\left(U-V\right) - \frac{1}{2} ord_p \frac{c}{a} - \frac{(n-3)}{2} ord_p b + \frac{(n-3)}{2} ord_p a\right]$$

$$= \frac{2}{n-1}\left[ord_p\left(U-V\right) - \frac{1}{2} ord_p \frac{cb^{(n-3)}}{a^{(n-2)}}\right]$$

Let $W=ord_p V=ord_p U$,

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

Therefore,

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

with $W=ord_p U = ord_p V$ 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, $ord_p b^2 > ord_p ac$, $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ and $ord_p s, ord_p t \ge \alpha > \delta$.

If $ord_p U = \frac{1}{2} ord_p \frac{s+\lambda_1 t}{na+\lambda_1 b}$ and $ord_p V = \frac{1}{2} ord_p \frac{s+\lambda_2 t}{na+\lambda_2 b}$ then $ord_p x \ge \frac{1}{n-1}(\alpha-(n-3)\delta)$ and $ord_p y \ge \frac{1}{n-1}(\alpha-(n-3)\delta)$.

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

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

Then,

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

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

From Theorems 2.2 and 2.3, we obtain that

$$ord_p x \geq \frac{2}{n-1} W \tag{1}$$

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

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

From (1),

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

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

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

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

Then, by hypothesis,

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

Now from (2),

$$ord_p y \geq \frac{2}{n-1}\left[W - \frac{1}{2} ord_p \frac{cb^{(n-3)}}{a^{(n-2)}}\right]$$

$$= \frac{2}{n-1}\left[\frac{1}{2} ord_p \frac{s+\lambda_2 t}{na+\lambda_2 b} - \frac{1}{2} ord_p \frac{c}{a} + \left(\frac{n-3}{2}\right) ord_p \frac{a}{b}\right]$$

$$\geq \frac{1}{n-1} ord_p \left(\frac{s+\lambda_2 t}{na+\lambda_2 b}\right) - \left(\frac{n-3}{n-1}\right)\left[ord_p \frac{b}{a} + ord_p c\right]$$

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

$$ord_p y \geq \frac{1}{n-1} ord_p (s+\lambda_i t) - \frac{1}{n-1} ord_p a + \left(\frac{n-3}{n-1}\right) ord_p a \,,$$

$$-\left(\frac{n-3}{n-1}\right)\max\{ord_p b, ord_p c\}$$

$$\geq \frac{1}{n-1}\left[ord_p (s+\lambda_i t) - (n-3)\max\{ord_p b, ord_p c\}\right], \ i = 1,2.$$

By the same method for $ord_p x$ from equation (3), we have

$$ord_p y \geq \frac{1}{n-1}\left(\alpha - (n-3)\delta\right).$$

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

$$ord_p a < ord_p \lambda_i b \,, \ i=1,2.$$

Therefore,

$$ord_p x \geq \frac{1}{n-1}(\alpha - \delta) \geq \frac{1}{n-1} ord_p \left(\alpha - (n-3)\delta\right) \text{ and } ord_p y \geq \frac{1}{n-1}(\alpha - (n-3)\delta)$$

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 $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b, ord_p c\}$ and $ord_p b^2 > ord_p ac$.

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

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

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

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

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

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

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

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

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)

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

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

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

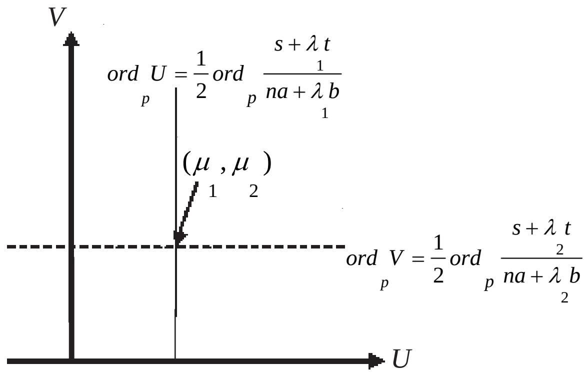

Figure 1: The indicator diagrams of $F(U,V) = (na + \lambda_1 b)U^2 + s + \lambda_1 t$ and $G(U,V) = (na + \lambda_2 b)V^2 + s + \lambda_2 t$.

From Figure 1 and Theorem 2.1 there exists $(\hat{U},\hat{V})$ in $\Omega_p \times \Omega_p$ such that $F(\hat{U},\hat{V}) = 0$, $G(\hat{U},\hat{V}) = 0$ and $ord_p \hat{U} = \mu_1$, $ord_p \hat{V} = \mu_2$ where $\mu_1 = \frac{1}{2} ord_p \frac{s+\lambda_1 t}{na+\lambda_1 b}$ and

$$\mu_2 = \frac{1}{2} ord_p \frac{s+\lambda_2 t}{na+\lambda_2 b}.$$

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

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

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

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

From Theorem 2.4, we have

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

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 $G(\hat{U},\hat{V}) = (g + \lambda_2 h)(\xi,\eta)$.

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

Also $G(\hat{U},\hat{V}) = 0$. Therefore $g(\xi,\eta) + \lambda_2 h(\xi,\eta) = 0$ (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, $ord_p \xi \geq \dfrac{1}{n-1}(\alpha - (n-3)\delta)$ and $ord_p \eta \geq \dfrac{1}{n-1}(\alpha - (n-3)\delta)$ where (ξ,η) are the zeros of g and h and $\delta = \max\{ord_p a, ordpb, ord_p c\}$.

We will get a sharper result if $ord_p a > ord_p b$, 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 $\alpha > 0$, $\delta = \max\{ord_p a, ord_p c\}, ord_p b^2 > ord_p ac$ and $ord_p a > ord_p b$.
If $ord_p f_x(0,0), ord_p f_y(0,0) \geq \alpha > \delta$ there exists (ξ,η) such that $f_x(\xi,\eta)=0, f_y(\xi,\eta)=0$ and

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

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

$$ord_p x_0 \geq \frac{1}{n-1}(\alpha - \delta),$$

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

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.