Pertanika J. Sci. & Technol. 15(1): 61 - 76 (2007)
ISSN: 0128-7680
© Universiti Putra Malaysia Press

A Method of Estimating the p-adic Sizes of Common Zeros of Partial Derivative Polynomials Associated with a Seventh Degree Form

Siti Hasana Sapar, Kamel Ariffin Mohd Atan & Mohamad Rushdan Md Said

Laboratory of Theoretical Mathematics, Institute for Mathematical Research
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia

Received: 28 July 2005

ABSTRAK

Katakan $\underline{x} = (x_1, x_2,...,x_n)$ vektor dalam ruang Z^n dengan Z menandakan gelanggang integer dan q integer positif, f polinomial dalam $\underline{x}$ dengan pekali dalam Z. Hasil tambah eksponen yang disekutukan dengan f ditakrifkan sebagai $S(f;q) = \Sigma\exp(2\pi i f(x)/q)$ yang dinilaikan bagi semua nilai x di dalam reja lengkap modulo q. Nilai $S(f,q)$ adalah bersandar kepada penganggaran bilangan unsur $|V|$, yang terdapat dalam set $V = \{\underline{x} \bmod q \mid f_{\underline{x}} \equiv \underline{0} \bmod q\}$ dengan $f_{\underline{x}}$ menandakan polinomial-polinomial terbitan separa f terhadap $\underline{x}$. Untuk menentukan kekardinalan bagi V, maklumat mengenai saiz p-adic pensifar sepunya perlu diperolehi. Makalah ini membincangkan suatu kaedah penentuan saiz p-adic bagi komponen (ξ,η) pensifar sepunya pembezaan separa $f(x,y)$ dalam $Z_p[x,y]$ berdarjah tujuh berasaskan teknik polihedron Newton yang disekutukan dengan polinomial terbabit. Polinomial berdarjah tujuh yang dipertimbangkan berbentuk $f(x,y) = ax^7 + bx^6y + cx^5y^3 + sx + ty + k$.

ABSTRACT

Let $\underline{x} = (x_1, x_2,...,x_n)$ be a vector in a space Z^n with Z ring of integers and let q be a positive integer, f a polynomial in x with coefficients in Z. The exponential sum associated with f is defined as $S(f;q) = \Sigma\exp(2\pi i f(x)/q)$ 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 $V = \{\underline{x} \bmod q \mid f_{\underline{x}} \equiv \underline{0} \bmod q\}$ where $f_{\underline{x}}$ is the partial derivative 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 $Z_p[x,y]$ of degree seven based on the p-adic Newton polyhedron technique associated with the polynomial. The seventh degree form considered is of the type $f(x,y) = ax7 + bx^6y + cx^5y^3 + sx + ty + k$.

Keywords: Partial derivative polynomials, seventh degree form, Newton polyhedron technique

INTRODUCTION

In our discussion, we use notation Z_p, Ω_p and $ord_p x$ to respectively denote the ring of p-adic integers, completion of the algebraic closure of Q_p the field of rational p-adic numbers and the highest power of p which divides x. For each prime p, let $f = (f_1, f_2,..., f_n)$ be an n-tuple polynomials in where $Z_p[\underline{x}]$ is the ring of p-adic integers and $\underline{x} = (x_1, x_2,..., x_n)$.

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

form $S(f;q) = \sum_{mod\ q} \exp\left(\frac{2\pi i f}{q}\right)$ where $f(\underline{x})$ is a polynomial in $Z(\underline{x})$ and the sum taken over a complete set of residues x modulo a positive integer q.

Loxton and Vaughn (1985) are among the researchers who investigate $S(f;q)$ where f is a non-linear polynomial in $Z(\underline{x})$. They find 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 $S(f;q)$ is found by other workers such as Mohd Atan (1986). He considered in particular the non-linear polynomial $f(x,y) = ax^3 + bx^2y + cx^5y^3 + cx + dy + e$. in which 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 $\delta = \max\{ord_p 3a, ord_p b, ord_p c, ord_p 3d\}$.

In 1997 Chan and Mohd Atan 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 (ξ,η) a root of $f(x,y)$, $ord_p\xi \geq \frac{1}{3}(\alpha - \delta)$ 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 derivative functions of the cubic form $f(x,y) = ax^3 + bx^2y + cx^2 + dy + e$.

In their work, they attempt to find a better estimation 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 in determining the p-adic sizes of the component (ξ,η) a common root of partial polynomial of $f(x,y)$ in $Z_p(x,y)$ of degree seven. The polynomial that is considered in this paper is of the form $f(x,y) = ax^7 + bx^5y + c^5y^2 + sx + ty + k$.

We will arrive at the desired estimate by examining the combinations of the indicator diagrams associated with the Newton polyhedrons of f_x and f_y. The following section gives a brief description of the polyhedron as developed by Mohd Atan and Loxton (1986). It is an analogue of the p-adic Newton polygon developed by Koblitz (1977).

NEWTON POLYHEDRON

Definition 2.1

Let p be a prime and $f(x,y) = \Sigma\, a_{ij}x^iy^j$ a polynomial in $Z_p[x,y]$. We map the term $T_{ij} = a_{ij}x^iy^j$ of $f(x,y)$ to the points $P_{ij} = (i,j,ord_p a_{ij})$ in the three dimensional Euclidean space and call this set of points Newton diagram of $f(x,y)$.

Below is an example of a Newton diagram for a lower degree polynomial.

Example 2.1:

Definition 2.2

Let p be a prime and $f(x,y) = (\ a_{ij}x^iy^j$ a polynomial in $\Omega_p[x,y]$. The Newton polyhedron of

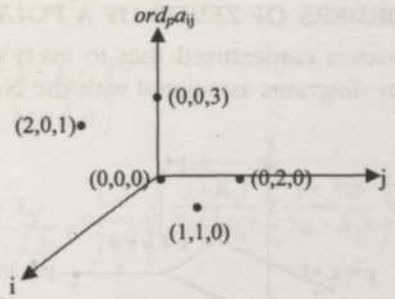


Fig. 1: Newton diagram of f(x,y) = 3x2 + 2xy (y2+27 with p = 3

$f(x,y)$ is the lower convex hull of the Newton diagram of $f(x,y)$. It is the highest convex connected surface which passes through or below the point P_{ij} in the Newton diagram of $f(x,y)$. If $a_{ij} = 0$ then the associated point is omitted since it lies at infinity above the i-j plane.

Below is the Newton polyhedron associated with the polynomial in Example 2.1.

Example 2.2:

Definition 2.3

Let $(\mu_s,\lambda_s,1)$ be the normalized upward-pointing normal to the faces Fi of N_f, the Newton

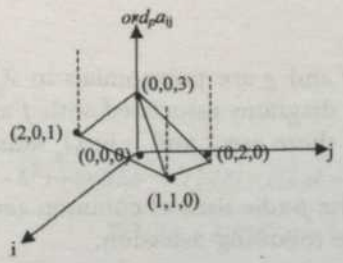


Fig. 2: The Newton polyhedron of f(x,y) = 3x² + 2xy (y²+27 with p = 3

polyhedron of a polynomial $f(x,y)$ in $Q_p[x,y]$. We map $(\mu_r,\lambda_r,1)$ to the points (μ_r,λ_r) in the x-y plane. If F_r and F_s are adjacent faces in N_f sharing a common edge, we construct the straight line joining (μ_r,λ_r) and (μ_s,λ_s). If F_r has a common edge with the vertical face F say $\alpha x + \beta y = \gamma$ in N_f, we construct the straight line segment joining (μ_r,λ_r) and the appropriate point at infinity that corresponds to the normal of F, that is the segment along a line with slope $-\alpha/\beta$. We call the set of lines, therefore obtained the indicator diagram associated with the Newton polyhedron of $f(x,y)$ (Mohd. Atan, 1986).

The indicator diagram associated with the Newton polyhedron in Example 2.2 is as shown in the following example.

Example 2.3 :

P-ADIC ORDERS OF ZEROS OF A POLYNOMIAL

In 1986 Mohd Atan and Loxton conjectured that to every point of intersection of the combination of the indicator diagrams associated with the Newton polyhedrons of a pair

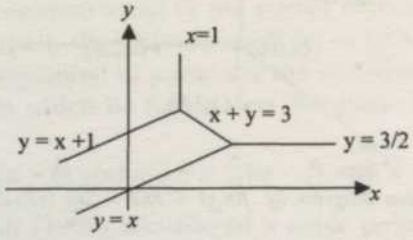


Fig. 3: Indicator diagram associated with the polynomial $f(x,y) = 3x^2 + 2xy - y^2+27$ with $p=3$

of polynomials in 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 proven by Mohd Atan and Loxton (1986). Sapar and Mohd Atan (2002) improved this result and is written as follows:

Theorem 3.1

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 and $f(\xi, \eta) = g(\xi, \eta) = 0$ and $ord_p\xi = \mu$, $ord_p\eta = \lambda$.

In Theorem 3.2 we give the p-adic sizes of common zeros of partial derivatives of the polynomial. First we have the following assertion:

Lemma 3.1

Let $p>7$ be an odd prime, a, b, c, s and t in Z_p. λ_1, λ_2 be the zeros of $k(x) = c^2x^2 - bcx = 9b^2 - 35ac$. If U, V are in Ω_p and $ord_p b^2 > ord_p ac$ with

$$ord_p U = \frac{1}{2}\, ord_p\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right) \text{ and } ord_p V = \frac{1}{2}\, ord_p\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)$$

then $ord_p(U + V) = ord_p(U - V)$.

Proof :

Let λ_1, λ_2 be the zeros of $k(x)= c^2x^2 + bcx + 9b^2 - 35ac$, where

$$\lambda_1 = \frac{-b+\sqrt{140ac-35b^2}}{2c}, \quad \lambda_1 = \frac{-b-\sqrt{140ac-35b^2}}{2c}, \quad U = u\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)^{1/2}$$

and $V = v\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)^{1/2}$, where $ord_p U = 0,\ ord_p v = 0$

$$U + V = u\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)^{1/2} + v\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)^{1/2}$$

$$(U+V)^2 = \left[\frac{s+\lambda_1 t}{7a+\lambda_1 b}u^2 + \frac{s+\lambda_2 t}{7a+\lambda 2b}v^2\right] + 2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda 2t}{7a+\lambda_2 b}\right)}uv \qquad (1)$$

Substituting λ_1, λ_2 in (1) and simplifying, we have

$$(U+V)^2 = \left[\frac{\left[sc(14ac-b^2)+bt(18b^2-77ac)+c(7at-bs)\sqrt{140ac-35b^2}\right]u^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right.$$

$$\left.+\frac{\left[sc(14ac-b^2)+bt(18b^2-77ac)+c(bs-7at)\sqrt{140ac-35b^2}\right]v^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right]$$

$$+ 2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv.$$

Thus,

$$ord_p(U+V) = \frac{1}{2}ord_p\left[\left[\frac{\left[sc(14ac-b^2)+bt(18b^2-77ac)+c(7at-bs)\sqrt{140ac-35b^2}\right]u^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right.\right.$$

$$\left.+\frac{\left[sc(14ac-b^2)+bt(18b^2-77ac)+c(bs-7at)\sqrt{140ac-35b^2}\right]v^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right]$$

$$\left.+ 2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv\right] \qquad (2)$$

Now consider,

$$U - V = u\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)^{1/2} - v\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)^{1/2}$$

$$(U+V)^2 = \left[\frac{s+\lambda_1 t}{7a+\lambda_1 b}u^2 + \frac{s+\lambda_2 t}{7a+\lambda_2 b}v^2\right] - 2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv$$

$$= \left[\frac{(s+\lambda_1 t)(7a+\lambda_2 tb)u^2 + (s+\lambda_2 t)(7a+\lambda_1 b)v^2}{(7a+\lambda_1 b)(7a+\lambda_2 b)}\right] - 2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv \quad (3)$$

Substituting λ_1, λ_2 in (3) and simplifying, we have

$$(U-V)^2 = -\left[\frac{\left[sc\left(b^2-14ac\right)+bt\left(77ac-18b^2\right)+c(bs-7at)\sqrt{140ac-35b^2}\right]u^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right.$$

$$\left. + \frac{\left[\left[sc\left(b^2-14ac\right)+bt\left(77ac-18b^2\right)+c(7at-bs)\sqrt{140ac-35b^2}\right]v^2\right]}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right]$$

$$-2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv.$$

Hence,

$$ord_p(U-V) = \frac{1}{2}ord_p\left[(-1)\left[\frac{\left[sc\left(b^2-14ac\right)+bt\left(77ac-18b^2\right)+c(bs-7at)\sqrt{140ac-35b}\right]u^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_1 b)}\right.\right.$$

$$\left.\left. + \frac{\left[sc\left(b^2-14ac\right)+bt\left(77ac-18b^2\right)+c(7at-bs)\sqrt{140ac-35b^2}\right]v^2}{2c^2(7a+\lambda_1 b)(7a+\lambda_2 b)}\right]\right.$$

$$\left. +2\sqrt{\left(\frac{s+\lambda_1 t}{7a+\lambda_1 b}\right)\left(\frac{s+\lambda_2 t}{7a+\lambda_2 b}\right)}uv\right]. \quad (4)$$

By (2) and (4) $ord_p(U+V) = ord_p(U-V)$, since $ord_p(14ac - b^2) = ord_p(b^2 - 14ac)$, $ord_p(77ac - 18b^2) = ord_p(18b^2 + 77ac)$ and $ord_p(7at - bs) = ord_p(bs - 7at)$.

In the following lemma, U and V are as in Lemma 3.1.

Lemma 3.2

Let U, V be as above, and $p>7$ be an odd prime, a, b and c in Z_p. λ_1, λ_2 be the zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$ and let

$$\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b} \text{ and } \alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b}.$$

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

$$ord_p(\alpha_1 V - \alpha_2 U) = ord_p \frac{\sqrt{140ac-35b^2}}{2c}[7ac - 3b^2](U+V) - ord_p(7a+\lambda_1 b) - ord_p(7a+\lambda_1 b).$$

Proof :

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

with $\lambda_1 = \frac{-b+\sqrt{140ac-35b^2}}{2c}$ and $\lambda_1 = \frac{-b-\sqrt{140ac-35b^2}}{2c}$ the zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$. Then

$$ord_p(\alpha_1 V - \alpha_2 U) = ord_p\left(\frac{3b+\lambda_1 c}{7a+\lambda_1 b}V - \frac{3b+\lambda_2 c}{7a+\lambda_2 b}U\right)$$

$$= ord_p[(3b+\lambda_1 c)(7a+\lambda_2 b)V - (3b+\lambda_2 c)(7a+\lambda_1 b)U].$$
$$ord_p(7a+\lambda_1 b) - ord_p(7a+\lambda_2 b) \quad (1)$$

Now,

$$(3b+\lambda_1 c)(7a+\lambda_2 b)V - (3b+\lambda_2 c)(7a+\lambda_1 b)U$$
$$= (21ab + 3b^2\lambda_2 + 7ac\lambda_1 + bc\lambda_1\lambda_2)V - (21ab + 3b^2\lambda_1 + 7ac\lambda_2 + bc\lambda_1\lambda_2)U$$
$$= (21ab + bc\lambda_1\lambda_2)(V+U) + (b^2\lambda_2 + 7ac\lambda_1)V - (3b^2\lambda_1 + 7ac\lambda_2)U \quad (2)$$

where λ_1, λ_2 as above. That is,

$$(3b+\lambda_1 c)(7a+\lambda_2 b)V - (3b+\lambda_2 c)(7a+\lambda_1 b)U$$
$$= \left(21ab + bc\left(\frac{-b+\sqrt{140ac-35b^2}}{2c}\right)\left(\frac{-b-\sqrt{140ac-35b^2}}{2c}\right)\right)(V-U)$$
$$+ \left[3b^2\left(\frac{-b+\sqrt{140ac-35b^2}}{2c}\right) + 7ac\left(\frac{-b-\sqrt{140ac-35b^2}}{2c}\right)\right]V$$
$$- \left[3b^2\left(\frac{-b+\sqrt{140ac-35b^2}}{2c}\right) + 7ac\left(\frac{-b-\sqrt{140ac-35b^2}}{2c}\right)\right]U \quad (3)$$

Simplifying equation (3), we obtain,

$$(3b + \lambda_1 c)(7a + \lambda_2 b)V - (3b + \lambda_2 c)(7a + \lambda_1 b)U = \frac{b}{2c}[15b^2-35ac](V-U)$$

$$+ \frac{\sqrt{140ac-35b^2}}{2c}[7ac-3b^2](U+V).$$

Since $p>7$ and $ord_p b^2 > ord_p ac$, we have

$$ord_p \frac{b}{2c}[15b^2-35ac](V-U) = ord_p b + ord_p ac + ord_p(V-U) - ord_p c \quad (4)$$

and

$$ord_p \frac{\sqrt{140ac-35b^2}}{2c}[7ac-3b^2](U+V) = \frac{1}{2}ord_p ac + ord_p ac + ord_p(V+U) - ord_p c. \quad (5)$$

Since $ord_p b > \frac{1}{2} ord_p ac$ and Lemma 3.1, we have from (4) and (5):

$$ord_p \frac{b}{2c}[15b^2-35ac](V-U) > ord_p \frac{\sqrt{140ac-35b^2}}{2c}[7ac-3b^2](U+V).$$

Thus,

$$ord_p[(3b+\lambda_1 c)(7a+\lambda_2 b)V - (3b+\lambda_2 c)(7a+\lambda_1 b)U] = ord_p \frac{\sqrt{140ac-35b^2}}{2c}[7ac-3b^2](U+V).$$

Therefore, from (1) we have

$$ord_p(\alpha_1 V - \alpha_2 U) = ord_p \frac{\sqrt{140ac-35b^2}}{2c}[7ac-3b^2](U+V) - ord_p(7a+\lambda_1 b) - ord_p(7a+\lambda_2 b).$$

Lemma 3.3

Let $p>7$ be an odd prime, a, b and c in Z_p. λ_1, λ_2 be the zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$ and let

$$\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b} \text{ and } \alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b}.$$

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 $i = 1, 2$.

Proof :

The zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$ are given by

$$\lambda_1 = \frac{-b+\sqrt{140ac-35b^2}}{2c} \text{ and } \lambda_2 = \frac{-b-\sqrt{140ac-35b^2}}{2c}.$$

Thus,

$$\lambda_1 c = \frac{-b+\sqrt{140ac-35b^2}}{2c}.$$

Since $ord_p b^2 > ord_p ac$, $p>7$, we have

$$ord_p \lambda_1 c = ord_p\left[\frac{-b+\sqrt{140ac-35b^2}}{2}\right] = \frac{1}{2} ord_p ac$$

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

Similarly it can be shown that $ord_p \lambda_2 c = \frac{1}{2} ord_p ac < ord_p b.$

Therefore, $ord_p(3b + \lambda_i c) = ord_p \lambda_i c = \frac{1}{2} ord_p ac$, $i = 1, 2.$ (1)

Now, consider

$$\lambda_1 b = b\left[\frac{-b+\sqrt{140ac-35b^2}}{2c}\right]$$

$$ord_p \lambda_1 b = ord_p b + ord_p\left[-b+\sqrt{140ac-35b^2}\right] - ord_p 2c.$$

Since $ord_p b > \frac{1}{2} ord_p ac$,

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

$$= ord_p a.$$

Thus, $ord_p \lambda_1 c > ord_p a.$

Similarly it can be shown that $ord_p \lambda_2 c > ord_p a.$
It follows that, $ord_p(7a + \lambda_i b) = ord_p a$, $i = 1,2$. (2)

From (1) and (2), and since $p>7$, we have

$$ord_p \alpha_i = ord_p\left(\frac{3b+\lambda_i c}{7a+\lambda_i b}\right),\ i = 1, 2$$

That is

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

$$= \frac{1}{2} ord_p \frac{c}{a}, \text{ for } i = 1, 2. \quad (3)$$

It can be shown that

$$\alpha_1 - \alpha_2 = \frac{(\lambda_1 - \lambda_2)(7ac - 3b^2)}{(7a + \lambda_1 b)(7a + \lambda_2 b)}$$

where, $\lambda_1 - \lambda_2 = \dfrac{\sqrt{140ac - 35b^2}}{c}$.

Thus, $ord_p(\alpha_1 - \alpha_2) = ord_p\sqrt{140ac - 35b^2} - ord_p c + ord_p(7ac - 3b^2)$
$-ord_p(7a + \lambda_1 b) - ord_p(7a + \lambda_2 b)$.

Since $p>7$, $ord_p b^2 > ord_p ac$ and by (2), we have

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

$$= \frac{1}{2}(ord_p c - ord_p a).$$

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

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

Lemma 3.4

Let $p>7$ be an odd prime, a, b, c, s and t in Z_p. Suppose that $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b\}$, and $ord_p s$, $ord_p t \geq \alpha > \delta$. Let γ, β be in Ω_p, λ_1 and λ_2 be the zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$ and

$$U = \gamma^3 + \frac{3b + \lambda_1 c}{7a + \lambda_1 c}\gamma^2\beta \text{ and } U = \gamma^3 + \frac{3b + \lambda_2 c}{7a + \lambda_2 c}\gamma^2\beta .$$

If $ord_p b^2 > ord_p ac$, $ord_p a > ord_p c$ and $ord_p U = \dfrac{1}{2} ord_p \dfrac{s + \lambda_1 t}{7a + \lambda_1 b}$, $ord_p V = \dfrac{1}{2} ord_p \dfrac{s + \lambda_2 t}{7a + \lambda_2 b}$ then

$ord_p \gamma \geq \dfrac{1}{6}(\alpha - \delta)$ and $ord_p \beta \geq \dfrac{1}{6}(\alpha - \delta)$.

Proof:

Let $\alpha_1 = \dfrac{3b + \lambda_1 c}{7a + \lambda_1 b}$ and $\alpha_2 = \dfrac{3b + \lambda_2 c}{7a + \lambda_2 b}$

with λ_1 and λ_2 zeros of $k(x) = c^2x^2 + bcx + 9b^2 - 35ac$. The expressions for λ_1, λ_2 are as given in the proof of Lemma 3.3. Then

$$U = \gamma^3 + \alpha_1\gamma^2\beta \quad (1)$$
$$V = \gamma^3 + \alpha_1\gamma^2\beta \quad (2)$$

By solving simultaneously (1) and (2) , we obtain

$$\gamma^3 = \frac{\alpha_1 V - \alpha_2 U}{\alpha_1 - \alpha_2} \tag{3}$$

If follows that,

$$3ord_p \gamma = ord_p (\alpha_1 V - \alpha_2 U) - ord_p (\alpha_1 - \alpha_2).$$

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

$$3ord_p \gamma \geq ord_p \alpha_1 V - ord_p (\alpha_1 - \alpha_2)$$
$$= ord_p \alpha_1 + ord_p V - ord_p V - ord_p (\alpha_1 - \alpha_2).$$

By Lemma 3.3, $ord_p \alpha_1 = ord_p (\alpha_1 - \alpha_2)$ and by its proof $ord_p (7a + \lambda_i b) = ord_p a$, $i = 1,2$.

Therefore

$$3ord_p \gamma \geq ord_p V.$$

That is,

$$3ord_p \gamma \geq \frac{1}{2} ord_p \left(\frac{s + \lambda_2 t}{7a + \lambda_2 b} \right)$$

$$= \frac{1}{2} [ord_p (s + \lambda_2 t) - ord_p a] \tag{4}$$

where $ord_p (s + \lambda_2 t) = ord_p [2cs + (-b - \sqrt{140ac - 35b^2}) t] - ord_p c$.

That is, $ord_p (s + \lambda_2 t) \geq \min \{ord_p 2cs, ord_p (-b - \sqrt{140ac - 35b^2}) t\} - ord_p c$.

Suppose $\min\{ord_p 2cs, ord_p (-b - \sqrt{140ac - 35b^2}) t\} = ord_p 2cs$. Then,

$$ord_p (s + \lambda_2 t) \geq ord_p 2cs - ord_p c.$$

That is, $ord_p (s + \lambda_2 t) \geq ord_p s.$ (5)

Hence, from (4) and (5).

$$3ord_p \gamma \geq \frac{1}{2} (ord_p (s - ord_p a).$$

Hence, by hypothesis,

$$ord_p \gamma \geq \frac{1}{6} (ord_p (s - ord_p a)$$

$$\geq \frac{1}{6} (\alpha - \delta).$$

Now, from (1) and (2), we will obtain

$$\beta = \frac{U-V}{(\alpha_1-\alpha_2)\gamma^2}.$$

Therefore ,

$$ord_p\beta = ord_p(U-V) - ord_p(\alpha_1-\alpha_2) - ord_p\gamma^2$$

with $ord_p\gamma = \frac{1}{3} ord_p \frac{\alpha_1 V - \alpha_2 U}{\alpha_1-\alpha_2}$ from (3). Then we have,

$$ord_p\beta = ord_p(U-V) - \frac{1}{3} ord_p(\alpha_1-\alpha_2) - \frac{2}{3} ord_p(\alpha_1 V - \alpha_2 U).$$

By Lemma 3.2, we obtain

$$ord_p\beta = ord_p(U-V) - \frac{1}{3} ord_p(\alpha_1-\alpha_2) + \frac{2}{3} ord_p(7a+\lambda_1 b) + \frac{2}{3} ord_p(7a+\lambda_2 b)$$

$$- \frac{2}{3} ord_p \frac{\sqrt{140ac-35b^2}}{2c} [7ac - 3b^2](U + V).$$

Since $ord_p b^2 > ord_p ac$, p>7 and from Lemma 3.1 and Lemma 3.3, we have

$$ord_p(U + V) - \frac{1}{3}\left(\frac{1}{2} ord_p \frac{c}{a}\right) + \frac{4}{3} ord_p a - \frac{2}{3}\left(\frac{1}{2} ord_p ac\right)$$

$$\frac{2}{3} ord_p ac + \frac{2}{3} ord_p c$$

$$\geq \frac{1}{3} \min\{ord_p U, ord_p V\} + \frac{1}{2} ord_p a - \frac{1}{2} ord_p c.$$

Suppose min $\{ord_p U, ord_p V\} = ord_p$, then

$$ord_p\beta \geq \frac{1}{3} ord_p V + \frac{1}{2} ord_p a - \frac{1}{2} ord_p c$$

$$= \frac{1}{6}[ord_p(s+\lambda_2 t) - ord_p(7a+\lambda_2 b) + ord_p a - 3ord_p a - 3ord_p c].$$

By equation (2) in proof of Lemma 3.3 and (5), we obtain

$$ord_p\beta \geq \frac{1}{6}[ord_p s - ord_p a + 3ord_p a - 3ord_p c].$$

Since $ord_p a > ord_p c$, we have

$$ord_p\beta \geq \frac{1}{6}[ord_p s - ord_p a]$$

$$\geq \frac{1}{6}(\alpha-\delta).$$

We will obtain the same result if

$\min\{ord_p 2cs, ord_p(-b-\sqrt{140ac-35b^2})t\} = ord_p(-b-\sqrt{140ac-35b^2})t$ and ,

$\min\{ord_p U, ord_p V\} = ord_p U$ for $ord_p\gamma$ and $ord_p\beta$.

Therefore, $ord_p\gamma \geq \frac{1}{6}(\alpha-\delta)$ and $ord_p\beta \geq \frac{1}{6}(\alpha-\delta)$.

Theorem 3.2

Let $f(x,y)=ax^7+bx^6y+cx^5y^2+sx+ty+k$ be a polynomial in $Z_p[x,y]$ with $p>7$. Let $\alpha > 0$, $\delta = \max\{ord_p a, ord_p b\}$, $ord_p a > ord_p c$ and $ord_p b^2 > ord_p ac$. If $ord_p f_x(0,0), ord_p f_y(0,0) \geq \alpha > \delta$ then there exists (ξ,η) such that $f_x(\xi,\eta)=0, f_y(\xi,\eta)=0$ and $ord_p \xi \geq \frac{1}{6}(\alpha-\delta)$.

Proof :

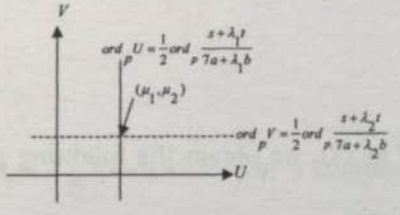


Fig. 4: The indicator diagrams of $F(U,V)=(7a+\lambda_1 b)U^2+s+\lambda_1 t$ and $G(U,V)=(7a+\lambda_1 b)V^2+\lambda_2 t$

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

Then,

$$(g+\lambda h(x,y)=(7a+\lambda b)x^6+(6b+2\lambda c)x^5y+5cx^4y^2+s+\lambda t$$

and

$$\frac{(g+\lambda h)(x,y)}{7a+\lambda b} = x^6+\left(\frac{6b+2\lambda c}{7a+\lambda b}\right)x^5y+\left(\frac{5c}{7a+\lambda b}\right)x^4y^2+\frac{s+\lambda t}{7a+\lambda b}. \quad (1)$$

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

$$\frac{(g+\lambda h)(x,y)}{7a+\lambda b}=\left(x^3+\frac{3b+\lambda c}{7a+\lambda b}x^2y\right)+\frac{s+\lambda t}{7a+\lambda b} \tag{2}$$

if

$$\frac{5c}{7a+\lambda b}-\left(\frac{3b+\lambda c}{7a+\lambda b}\right)^2=0.$$

That is $c^2x^2+bcx+9b^2-35ac=0$. (3)

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

$$\lambda_1=\frac{-b+\sqrt{35(4ac-b^2)}}{2c} \quad \text{and} \quad \lambda_2=\frac{-b+\sqrt{35(4ac-b^2)}}{2c}.$$

Now, let

$$U=x^3+\frac{3b+\lambda_1 c}{7a+\lambda_1 b}x^2y, \tag{4}$$

$$V=x^3+\frac{3b+\lambda_2 c}{7a+\lambda_2 b}x^2y, \tag{5}$$

$$F(U,V)=(g+\lambda_2 h)(x,y) \tag{6}$$

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)

$$F(U,V)=(7a+\lambda_1 b)U^2+s+\lambda_1 t \tag{8}$$

$$G(U,V)=(7a+\lambda_1 b)V^2+\lambda_2 t. \tag{9}$$

The combination of the indicator diagrams associated with the Newton polyhedron of (8) and (9) takes the form shown in the figure below:

From Figure 4 and Theorem 3.1 there exists $(\hat{U},\hat{V})$ such that $F_1(\hat{U},\hat{V})=0$, $G_1(\hat{U},\hat{V})=0$ and $ord_p\,\hat{U}=\mu_1$, $ord_p\,\hat{V}=\mu_2$ with $\mu_1=\frac{1}{2}ord_p\frac{s+\lambda_1 t}{7a+\lambda_1 b}$. Also from (4) and (5) there exists (x_0,y_0) such that

$$\hat{U}=x_0^3+\alpha_1 x_0^2 y_0 \text{ and } \hat{V}=x_0^3+\alpha_2 x_0^2 y_0$$

with $\alpha_1 = \frac{3b+\lambda_1 c}{7a+\lambda_1 b}, \alpha_2 = \frac{3b+\lambda_2 c}{7a+\lambda_2 b}$ in which λ_1, λ_2 are zeros of

$k(x)=c^2x^2 + bcx + 9b^2-35ac.$

In fact, $x_0 = \left(\frac{\alpha_1 \hat{V} - \alpha_2 \hat{U}}{\alpha_1 - \alpha_2}\right)^{1/3}$ and $y_0 = \frac{\hat{U} - \hat{V}}{(\alpha_1 - \alpha_2)^{1/3}(\alpha_1 V - \alpha_2 \hat{U})^{2/3}}$, where from Lemma 3.2,

$\alpha_1 \hat{V} - \alpha_2 \hat{U} \neq 0$ and from Lemma 3.3, $\alpha_1 - \alpha_2 \neq 0$.

From Lemma 3.4 and hypothesis, we see that

$$ord_p x_0 \geq \frac{1}{6}(\alpha-\delta) \quad \text{and} \quad ord_p y_0 \geq \frac{1}{6}(\alpha-\delta).$$

We have, from (6) and (7),

$$F_1(\hat{U},\hat{V}) = (g + \lambda_1 h)(x_0,y_0) \text{ and } G_1(\hat{U},\hat{V}) = (g + \lambda_2 h)(x_0,y_0).$$

Since $F_1(\hat{U},\hat{V}) = 0$, it follows that $g(x_0,y_0) + \lambda_1 h(x_0,y_0) = 0.$ (10)

Also since $G_1(\hat{U},\hat{V}) = 0$, $g(x_0,y_0) + \lambda_2 h(x_0,y_0) = 0.$ (11)

From (10) and (11), $(\lambda_1 - \lambda_2) h(x_0,y_0) = 0$. Since $\lambda_1 \neq \lambda_2$, we have $h(x_0,y_0)$. Similarly $g(x_0,y_0) = 0$.

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

Thus $ord_p \xi \geq \frac{1}{6}(\xi,\eta)$ and $ord_p \eta \geq \frac{1}{6}(\alpha-\delta)$ with (ξ,η) a common zero of g and h.

CONCLUSION

Our investigation finds that if p is an odd prime, $p > 7$, $f(x,y) = ax^7 + bx^6y + cx^5y^2 + sx + ty + k$ polynomial in $Z_p[x,y]$ with $ord_p b^2 > ord_p ac$ and $ord_p a > ord_p c$, then the p-adic sizes of common zeros of partial derivatives of this polynomial is $ord_p \xi \geq \frac{1}{6}(\alpha-\delta)$ and $ord_p \eta \geq \frac{1}{6}(\alpha-\delta)$ with $\alpha > \delta$ and $\delta = \max\{ord_p a, ord_p b\}$.

REFERENCES

CHAN, K.L. and MOHD. ATAN, K.A. (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 MOHD ATAN, K.A. (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 VAUGHN, R.C. (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 LOXTON, J.H. (1986). Newton polyhedral and solutions of congruences. In J.H. Loxton and A. Van der Poorten (Eds.), *Diophantine Analysis.* Cambridge: Cambridge University Press.

MOHD ATAN, K.A. and ABDULLAH, I.B. (1992). Set of solution to congruences equations associated with cubic form. *Journal of Physical Science, 3,*1-6.

SAPAR, S.H. and MOHD ATAN, K.A. (2002). Estimate for the cardinality of the set of solution to congruence equations (Malay). *Journal of Technology, (36C),* 13-40.