Proceedings of the 2nd IMT-GT Regional Conference on Mathematics, Statistics and Applications
Universiti Sains Malaysia

ON THE CARDINALITY OF THE SET OF SOLUTIONS TO CONGRUENCE EQUATION ASSOCIATED WITH QUINTIC FORM

Siti Hasana Sapar, Kamel Ariffin Mohd Atan and Muhamad Rushdan Md Said
Laboratory of Theoretical Mathematics, Institute for Mathematical Research, Universiti Putra Malaysia
sitihas@fsas.upm.edu.my, kamel@inform.upm.edu.my, mrushdan@inform.upm.edu.my

Abstract. 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 and let $\underline{x} = (x_1, x_2, ..., x_n)$ be a vector in the space Z^n with Z ring of integers and q be a positive integer, f a polynomial in $\underline{x}$ with coefficients in Z. 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

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

where $\underline{f}_{\underline{x}}$ is the partial derivative of f with respect to $\underline{x} = (x_1, x_2, ..., x_n)$. This paper will give an explicit estimate of $|V|$ for polynomial $f(x, y)$ in $Z_p[x, y]$ of degree five. Earlier authors have investigated similar polynomials of lower degrees. The polynomial that we consider in this paper is as follows:

$$f(x, y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k$$

The approach is by using p-adic Newton Polyhedron technique associated with this polynomial.

1. Introduction

In our discussion, we use notation Z_p, Ω_p and $ord_p x$ to denote respectively 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 $\underline{f} = (f_1, f_2, ..., f_n)$ be an n-tuple polynomials in $Z_p[\underline{x}]$ where Z_p is the ring of p-adic integers and $\underline{x} = (x_1, x_2, \ldots, x_n)$.

Loxton and Vaughn are among the researchers who investigate $S(f;q)$ where f is a non-linear polynomial in $Z[\underline{x}]$. They find that the estimation 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 estimations of $S(f;q)$ are found by other workers such as Mohd Atan(1986), Chan Kait Loon(1997) and Heng Swee Huay(1999) for lower degree polynomials. However, the general results for polynomials of several variables are less complete.

2. 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 of polynomials in $Z_p[\underline{x}]$ 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 Newton polyhedron of f and g. Then there are ξ and η in Ω_p satisfying

$$f(\xi, \eta) = g(\xi, \eta) = 0$$

and

$$\mathrm{ord}_p\, \xi = \mu, \quad \mathrm{ord}_p\, \eta = \lambda.$$

A special case of this conjecture was proved by Mohd Atan and Loxton (1986). Sapar and Mohd Atan (2002) improved this result and is written 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 Newton polyhedron of 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

$$\mathrm{ord}_p\, \xi = \mu, \quad \mathrm{ord}_p\, \eta = \lambda.$$

In Theorem 2.2 we give the p-adic sizes of common zeros of partial derivatives of the polynomial

$$f(x,y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k.$$

Theorem 2.2. *Let*

$$f(x,y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k$$

be a polynomial in $Z_p[x,y]$ with $p > 5$. Let

$$\alpha > 0,$$
$$\delta = \max\{\mathrm{ord}_p\, a, \mathrm{ord}_p\, b, \mathrm{ord}_p\, c, \mathrm{ord}_p\, d, \mathrm{ord}_p\, e, \mathrm{ord}_p\, m\},$$
$$\mathrm{ord}_p(10cm - 2de)^2 > \mathrm{ord}_p(10dm - 4e^2)(2ce - d^2),$$

and

$$\mathrm{ord}_p\, b^2 > \mathrm{ord}_p\, ac.$$

If

$$f_x(x_0,y_0), f_y(x_0,y_0) \geq \alpha > \delta$$

than there exist (ξ,η) such that

$$f_x(\xi,\eta) = 0, \quad f_y(\xi,\eta) = 0$$

and

$$\mathrm{ord}_p(\xi - x_0) \geq \frac{1}{4}(\alpha - \delta), \quad \mathrm{ord}_p(\eta - y_0) \geq \frac{1}{4}(\alpha - \delta).$$

Proof. Let

$$X = x - x_0, \quad Y = y - y_0$$

and

$$g(X + x_0, Y + y_0) = f_x(X + x_0, Y + y_0),$$
$$h(X + x_0, Y + y_0) = f_y(X + x_0, Y + y_0)$$

and λ be a constant. Then,

$$\begin{aligned}
&(g + \lambda h)(X + x_0, Y + y_0)\\
&= (5a + \lambda b)(X + x_0)^4 + (4b + 2\lambda c)(X + x_0)^3(Y + y_0)\\
&+ (3c + 3\lambda d)(X + x_0)^2(Y + y_0)^2 + (2d + 4\lambda e)(X + x_0)(Y + y_0)^3\\
&+ (e + 5\lambda m)(Y + y_0)^4 + s + \lambda t
\end{aligned}$$

and

$$\begin{aligned}
&\frac{(g + \lambda h)(X + x_0, Y + y_0)}{5a + \lambda b}\\
&= (X + x_0)^4 + \left(\frac{4b + 2\lambda c}{5a + \lambda b}\right)(X + x_0)^3(Y + y_0)\\
&+ \left(\frac{3c + 3\lambda d}{5a + \lambda b}\right)(X + x_0)^2(Y + y_0)^2 + \left(\frac{2d + 4\lambda e}{5a + \lambda b}\right)(X + x_0)(Y + y_0)^3\\
&+ \left(\frac{e + 5\lambda m}{5a + \lambda b}\right)(Y + y_0)^4 + \frac{s + \lambda t}{5a + \lambda b}
\end{aligned} \tag{2.1}$$

Let α_{ij} denote the coefficients of X^iY^j in the completed quartic form of the equation (2.1), $0 \leq i \leq 4, 0 \leq j \leq 4$. By completing the quartic equation (2.1) and by solving simultaneously equations $\alpha_{ij}(\lambda) = 0$, $i \neq 0$, $j \neq 0$ and $i + j = 4$, we obtain

$$\begin{aligned}
\frac{(g + \lambda h)(X + x_0, Y + y_0)}{5a + \lambda b} &= \left((X + x_0) + \frac{4b + 2\lambda c}{4(5a + \lambda b)}(Y + y_0)\right)^4 + \frac{s + \lambda t}{5a + \lambda b}\\
&= \left(\left(X + \frac{4b + 2\lambda c}{4(5a + \lambda b)}Y\right) + \left(x_0 + \frac{4b + 2\lambda c}{4(5a + \lambda b)}y_0\right)\right)^4\\
&+ \frac{s + \lambda t}{5a + \lambda b}
\end{aligned} \tag{2.2}$$

where λ satisfies the equation

$$\frac{e+5\lambda m}{5a+\lambda b}-\frac{1}{2}\frac{(d+2\lambda e)^2}{(c+\lambda d)(5a+\lambda b)}=0.$$

That is,

$$(10dm-4e^2)\lambda^2+(10cm-2de)\lambda+2ce-d^2=0. \tag{2.3}$$

From (2.3), we will obtain two values of λ, say λ_1, λ_2 where

$$\lambda_1=\frac{-(10cm-4e^2)+\sqrt{(10cm-2de)^2-4(10dm-4e^2)(2ce-d^2)}}{2(10dm-4e^2)}$$

and

$$\lambda_2=\frac{-(10cm-4e^2)-\sqrt{(10cm-2de)^2-4(10dm-4e^2)(2ce-d^2)}}{2(10dm-4e^2).}$$

Now, let

$$U=X+\frac{4b+2\lambda_1 c}{4(5a+\lambda_1 b)}Y, \qquad u_0=x_0+\frac{4b+2\lambda_1 c}{4(5a+\lambda_1 b)}y_0 \tag{2.4}$$

$$V=X+\frac{4b+2\lambda_2 c}{4(5a+\lambda_2 b)}Y, \qquad v_0=x_0+\frac{4b+2\lambda_2 c}{4(5a+\lambda_2 b)}y_0. \tag{2.5}$$

By substitution of U and V in (2.2), we obtain the following polynomials in (U,V),

$$F(U,V)=(5a+\lambda_1 b)(U+u_0)^4+s+\lambda_1 t \tag{2.6}$$

and

$$G(U,V)=(5a+\lambda_2 b)(V+v_0)^4+s+\lambda_2 t. \tag{2.7}$$

From (2.6) and (2.7),we have

$$F(U,V)=(5a+\lambda_1 b)\left[U^4+4u_0U^3+6{u_0}^2U^2+4{u_0}^3U\right]+F_0 \tag{2.8}$$

$$G(U,V)=(5a+\lambda_2 b)\left[V^4+4v_0V^3+6{v_0}^2V^2+4{v_0}^3V\right]+G_0 \tag{2.9}$$

where

$$F_0=f_x(x_0,y_0)+\lambda_1 f_y(x_0,y_0)$$

and

$$G_0=f_x(x_0,y_0)+\lambda_2 f_y(x_0,y_0).$$

The combination of the indicator diagrams associated with the Newton polyhedron of (2.8) and (2.9) takes the form shown in Figure 2.1 below:

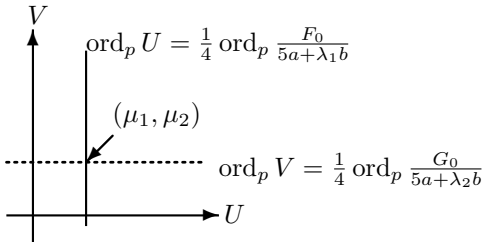

Figure 2.1. The indicator diagrams of$F(U,V)=(5a+\lambda_1 b)U^2+F_0$ and $G(U,V)=(5a+\lambda_2 b)V^2+G_0$

From Figure 2.1 and Theorem 2.1 there exists $(\hat{U},\hat{V})$ in ${\Omega_p}^2$ such that

$$F_1\left(\hat{U},\hat{V}\right)=0, G_1\left(\hat{U},\hat{V}\right)=0$$

and

$$\operatorname{ord}_p\hat{U}=\mu_1, \quad \operatorname{ord}_p\hat{V}=\mu_2$$

with

$$\mu_1 = \frac{1}{4}\operatorname{ord}_p \frac{F_0}{5a+\lambda_1 b} \quad and \quad \mu_2 = \frac{1}{4}\operatorname{ord}_p \frac{G_0}{5a+\lambda_2 b}.$$

Suppose $U = \hat{U}$ and $V = \hat{V}$ in (2.4) and (2.5) there exists (X_0, Y_0) such that

$$\hat{U} = X_0 + \alpha_1 Y_0 \quad and \quad \hat{V} = X_0 + \alpha_2 Y_0$$

with

$$\alpha_1 = \frac{4b + 2\lambda_1 c}{4(5a+\lambda_1 b)}, \quad \alpha_2 = \frac{4b+2\lambda_2 c}{4(5a+\lambda_2 b)}$$

in which λ_1, λ_2 are zeros of

$$k(\lambda) = (10dm - 4e^2)\lambda^2 + (10cm - 2de)\lambda + 2ce - d^2.$$

Solving for X_0 and Y_0 we obtain

$$X_0 = \frac{\alpha_2\hat{U} - \alpha_1\hat{V}}{\alpha_2 - \alpha_1} \quad and \quad Y_0 = \frac{\hat{U}-\hat{V}}{\alpha_1 - \alpha_2}.$$

Then,

$$\operatorname{ord}_p X_0 = \operatorname{ord}_p(\alpha_1\hat{V} - \alpha_2\hat{U}) - \operatorname{ord}_p(\alpha_1 - \alpha_2).$$

with

$$\operatorname{ord}_p(\alpha_1 - \alpha_2) = \operatorname{ord}_p \frac{(2b^2 - 5ac)(\lambda_2 - \lambda_1)}{2(5a+\lambda_1 b)(5a+\lambda_2 b)}$$

and

$$\lambda_2 - \lambda_1 = -\frac{\sqrt{(10cm-2de)^2 - 4(10dm-4e^2)(2ce-d^2)}}{10dm - 4e^2}$$

since

$$\operatorname{ord}_p(10cm - 2de)^2 > \operatorname{ord}_p(10dm - 4e^2)(2ce - d^2),$$

we have

$$\operatorname{ord}_p(\lambda_2 - \lambda_1) = \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2}.$$

Therefore,

$$\begin{aligned}\operatorname{ord}_p X_0 &= \operatorname{ord}_p(\alpha_2\hat{U} - \alpha_1\hat{V}) - \operatorname{ord}_p \frac{(2b^2-5ac)(\lambda_2-\lambda_1)}{2(5a+\lambda_1 b)(5a+\lambda_2 b)} \\ &\geq \operatorname{ord}_p \hat{U} + \operatorname{ord}_p \frac{4b+2\lambda_2 c}{4(5a+\lambda_2 b)} - \operatorname{ord}_p \frac{(2b^2-5ac)(\lambda_2-\lambda_1)}{2(5a+\lambda_1 b)(5a+\lambda_2 b)}.\end{aligned}$$

Then, we have

$$\begin{aligned}\operatorname{ord}_p X_0 \geq{}& \operatorname{ord}_p \hat{U} + \operatorname{ord}_p(2b+\lambda_2 c) - \operatorname{ord}_p(2b^2-5ac) - \operatorname{ord}_p(\lambda_2-\lambda_1) \\ &+ \operatorname{ord}_p(5a+\lambda_1 b) \\ ={}& \frac{1}{4}\operatorname{ord}_p \frac{F_0}{5a+\lambda_1 b} + \operatorname{ord}_p(2b+\lambda_2 c) - \operatorname{ord}_p(2b^2-5ac) \\ &- \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} + \operatorname{ord}_p(5a+\lambda_1 b)\end{aligned}$$

Suppose

$$\begin{aligned}\min\{\operatorname{ord}_p 2b, \operatorname{ord}_p \lambda_2 c\} &= \operatorname{ord}_p b, \\ \min\{\operatorname{ord}_p 5a, \operatorname{ord}_p \lambda_1 b\} &= \operatorname{ord}_p \lambda_1 b\end{aligned}$$

and since

$$\operatorname{ord}_p b^2 > \operatorname{ord}_p ac,$$

we have

$$\operatorname{ord}_p X_0 \geq \frac{1}{4}\operatorname{ord}_p \frac{F_0}{5a+\lambda_1 b} + \operatorname{ord}_p b - \operatorname{ord}_p b^2 - \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} + \operatorname{ord}_p \lambda_1 b$$

since

$$\operatorname{ord}_p(10cm - 2de)^2 > \operatorname{ord}_p(10dm - 4e^2)(2ce - d^2),$$

we have

$$\begin{aligned}\operatorname{ord}_p X_0 &\geq \frac{1}{4}\operatorname{ord}_p \frac{F_0}{5a+\lambda_1 b} - \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} + \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} \\ &= \frac{1}{4}\operatorname{ord}_p \frac{f_x(x_0,y_0)+\lambda_1 f_y(x_0,y_0)}{5a+\lambda_1 b}.\end{aligned}$$

Suppose

$$\min\{\operatorname{ord}_p f_x(x_0,y_0), \operatorname{ord}_p \lambda_1 f_y(x_0,y_0)\} = \operatorname{ord}_p f_x(x_0,y_0)$$

and

$$\min\{\operatorname{ord}_p 5a, \operatorname{ord}_p \lambda_1 b\} = \operatorname{ord}_p \lambda_1 b,$$

we have

$$\begin{aligned}\operatorname{ord}_p X_0 &\geq \frac{1}{4}\left(\operatorname{ord}_p f_x(x_0,y_0) - \operatorname{ord}_p \lambda_1 b\right) \\ &\geq \frac{1}{4}\left(\operatorname{ord}_p f_x(x_0,y_0) - \operatorname{ord}_p a\right).\end{aligned}$$

Hence, by hypothesis,

$$\operatorname{ord}_p X_0 \geq \frac{1}{4}\left(\alpha-\delta\right).$$

Now,

$$Y_0 = \frac{\hat{U}-\hat{V}}{\alpha_1-\alpha_2}.$$

And hence,

$$\operatorname{ord}_p Y_0 = \operatorname{ord}_p(\hat{U}-\hat{V}) - \operatorname{ord}_p \frac{(2b^2-5ac)(\lambda_2-\lambda_1)}{2(5a+\lambda_1 b)(5a+\lambda_2 b)}.$$

Suppose

$$\min\{\operatorname{ord}_p \hat{U}, \operatorname{ord}_p \hat{V}\} = \operatorname{ord}_p \hat{U}$$

and since

$$\operatorname{ord}_p(5a+\lambda_1 b) = \operatorname{ord}_p(5a+\lambda_2 b),$$

we have

$$\begin{aligned}\operatorname{ord}_p Y_0 &\geq \operatorname{ord}_p \hat{U} - \operatorname{ord}_p(2b^2-5ac) - \operatorname{ord}_p(\lambda_2-\lambda_1) + 2\operatorname{ord}_p(5a+\lambda_1 b) \\ &= \frac{1}{4}\operatorname{ord}_p(f_x(x_0,y_0)+\lambda_1 f_y(x_0,y_0)) - \operatorname{ord}_p ac - \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} \\ &+ \frac{7}{4}\operatorname{ord}_p(5a+\lambda_1 b).\end{aligned}$$

Suppose

$$\min\{\operatorname{ord}_p 5a, \operatorname{ord}_p \lambda_1 b\} = \operatorname{ord}_p \lambda_1 b$$

and since $\operatorname{ord}_p b^2 > \operatorname{ord}_p ac$, we have

$$\begin{aligned}\operatorname{ord}_p Y_0 &\geq \frac{1}{4}\operatorname{ord}_p\left(f_x\left(x_0,y_0\right)+\lambda_1 f_y\left(x_0,y_0\right)\right) - \operatorname{ord}_p b^2 - \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} \\ &+ \frac{7}{4}\operatorname{ord}_p b + \frac{7}{4}\left(\frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2}\right) \\ &\geq \frac{1}{4}\operatorname{ord}_p\left(f_x\left(x_0,y_0\right)+\lambda_1 f_y\left(x_0,y_0\right)\right) - \frac{1}{4}\operatorname{ord}_p b - \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} \\ &+ \frac{1}{2}\operatorname{ord}_p \frac{2ce-d^2}{10dm-4e^2} \\ &\geq \frac{1}{4}\left(\operatorname{ord}_p\left(f_x\left(x_0,y_0\right)+\lambda_1 f_y\left(x_0,y_0\right)\right) - \operatorname{ord}_p b\right).\end{aligned}$$

Hence, by hypothesis,

$$\operatorname{ord}_p Y_0 \geq \frac{1}{4}(\alpha-\delta).$$

We will get the same result if

$$\begin{gathered}\min\{\operatorname{ord}_p 2b, \operatorname{ord}_p \lambda_2 c\} = \operatorname{ord}_p \lambda_2 c, \\ \min\{\operatorname{ord}_p 5a, \operatorname{ord}_p \lambda_1 b\} = \operatorname{ord}_p a\end{gathered}$$

and

$$\min\{\mathrm{ord}_p\, f_x(x_0,y_0), \mathrm{ord}_p\, \lambda_1 f_y(x_0,y_0)\} = \mathrm{ord}_p\, \lambda_1 f_y(x_0,y_0).$$

Suppose

$$\xi = X_0 + x_0 \quad and \quad \eta = Y_0 + y_0,$$

then

$$X_0 = \xi - x_0 \quad and \quad Y_0 = \eta - y_0.$$

Thus, we have

$$\mathrm{ord}_p\,(\xi - x_0) \geq \frac{1}{4}(\alpha - \delta) \quad and \quad \mathrm{ord}_p\,(\eta - y_0) \geq \frac{1}{4}(\alpha - \delta).$$

By back substitution in (2.6) and (2.7) and since $\lambda_1 \neq \lambda_2$ we have

$$g\,(\xi,\eta) = f_x\,(\xi,\eta) = 0$$

and

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

Thus,

$$\mathrm{ord}_p\,(\xi - x_0) \geq \frac{1}{4}(\alpha - \delta)$$

and

$$\mathrm{ord}_p\,(\eta - y_0) \geq \frac{1}{4}(\alpha - \delta)$$

with (ξ,η) a common zero of g and h. □

2.1. Cardinality of $V(g,h;p^\alpha)$. Let p be a prime and $g(x,y)$, $h(x,y)$ polynomials in Z_p[x,y] and (ξ_i,η_i) common zeros of g and h. Let $\alpha > 0$,

$$H_i(\alpha) = \{(x,y) \in \Omega_p \times \Omega_p : \mathrm{ord}_p(x-\xi_i), \mathrm{ord}_p(y-\eta_i) = \max_j\{\mathrm{ord}_p(x-\xi_i), \mathrm{ord}_p(y-\eta_i)\}$$

and

$$\mathrm{ord}_p\, g(x,y), \mathrm{ord}_p\, h(x,y) \geq \alpha.$$

By the method of Loxton and Smith (1982), we can show that the value of |V(g,h;p^α)|, the cardinality of $V(g,h;p^\alpha)$ depends on $\mathrm{ord}_p(x-\xi_i), \mathrm{ord}_p(y-\eta_i)$with $(x,y) \in H_i(\alpha)$ as shown by Mohd Atan (1986) for polynomials of $n \geq 2$ variables. We state the theorem as follow:

Theorem 2.3. *Let p be a prime and $g(x,y)$, $h(x,y)$ two polynomials in $Z_p[x,y]$. Let $\alpha > 0, (\xi_i,\eta_i)$, $i \geq 1$ be common zeros of g and h, and*

$$\gamma_i(\alpha) = \inf_{x \in H(\alpha)}\{\mathrm{ord}_p(x-\xi_i), \mathrm{ord}_p(y-\eta_i)\}$$

where

$$H(\alpha) = \bigcup_i H_i(\alpha).$$

If $\alpha > \gamma_i(\alpha)$, then

$$|V(g,h;p^\alpha)| \leq \sum_i p^{2(\alpha-\gamma_i(\alpha))}.$$

By using Theorem (2.3) the following theorem gives the estimate to the cardinality $V(g,h;p^\alpha)$ associated with $g = f_x, h = f_y$ with $f(x,y)$ polynomials in $Z_p[x,y]$ of degree five.

Theorem 2.4. *Let $p > 5$ and*

$$f(x,y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k$$

be a polynomial in $Z_p[x,y]$. Suppose $\alpha > 0$,

$$\mathrm{ord}_p(10cm - 2de)^2 > \mathrm{ord}_p(10dm - 4e^2)(2ce - d^2),$$

$$\mathrm{ord}_p\, b^2 > \mathrm{ord}_p\, ac$$

and

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

Then,

$$|V(f_x, f_y; p^\alpha)| \leq \begin{cases} p^{2\alpha} & (\alpha \leq \delta) \\ 16p^{\frac{1}{3}(3\alpha+\delta)} & (\alpha > \delta). \end{cases}$$

Proof. Clearly $|V(f_x, f_y; p^\alpha)| \leq p^{2\alpha}$ if $\alpha \leq \delta$. Suppose now $\alpha > \delta$.

From Theorem 2.3

$$|V(g, h; p^\alpha)| \leq \sum_i p^{2(\alpha - \gamma_i(\alpha))}$$

with

$$\gamma_i(\alpha) = \inf_{x \in H(\alpha)} \{\mathrm{ord}_p(x - \xi_i), \mathrm{ord}_p(y - \eta_i)\}$$

where

$$H(\alpha) = \bigcup_i H_i(\alpha)$$

and

$$g = f_x, \qquad h = f_y.$$

From Theorem 2.2,

$$\gamma_i(\alpha) \geq \frac{1}{4}(\alpha - \delta).$$

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

$$|V(f_x, f_y; p^\alpha)| \leq 16p^{\frac{1}{2}(3\alpha+\delta)} \quad if \quad \alpha > \delta$$

Hence,

$$|V(f_x, f_y; p^\alpha)| \leq \begin{cases} p^{2\alpha} & (\alpha \leq \delta) \\ 16p^{\frac{1}{3}(3\alpha+\delta)} & (\alpha > \delta) \end{cases}$$

□

3. Conclusion

Our investigation finds that if p is prime, $p > 5$,

$$f(x, y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k$$

is a polynomial in $Z_p[x, y]$, $\alpha > 0$,

$$\mathrm{ord}_p(10cm - 2de)^2 > \mathrm{ord}_p(10dm - 4e^2)(2ce - d^2)$$

and

$$\mathrm{ord}_p\, b^2 > \mathrm{ord}_p\, ac,$$

then the cardinality for the set of

$$V = \{(x, y) \bmod p^\alpha \,|f_x(x, y), f_y(x, y) \equiv 0 \bmod p^\alpha\}$$

associated with $f(x, y)$ is :

$$|V(f_x, f_y; p^\alpha)| \leq \begin{cases} p^{2\alpha} & (\alpha \leq \delta) \\ 16p^{\frac{1}{3}(3\alpha+\delta)} & (\alpha > \delta) \end{cases}$$

with $\alpha > \delta$ and

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

This cardinality is useful in finding the estimate for exponential sums associated with such a polynomial.

References

[1] J. H. Loxton and R. A. Smith, Estimate for multiple exponential sums, *J. Aust. Math. Soc.* **33** (1982), 125–134.
[2] J. H. Loxton and R. C. Vaughn, The estimate of complete exponential sums, *Canad. Math Bull.* **28**(2)(1985), 440–454 .
[3] K. A. Mohd. Atan, Newton polyhedral method of determining p-adic orders of zeros common to two polynomials in $Q_p[x, y]$, *Pertanika* **9**(3) (1986), 375–380. Universiti Pertanian Malaysia.
[4] K. A. Mohd. Atan and J. H. Loxton, Newton polyhedra and solutions of congruences, *in:* Loxton, J.H. and Van der Poorten, A.(ed). Diophantine Analysis. Cambridge University Press, Cambridge, 1986.
[5] K. A. Mohd Atan and I. B Abdullah, Set of solution to congruences equations associated with cubic form, *J. Physical Sci.* **3** (1992), 1–6.
[6] K. L. Chan and K. A. Mohd. Atan, On the estimate to solutions of congruence equations associated with a quartic form, *J. Physical Sci.* **8** (1997), 21–34.
[7] S. H. Heng and K. A. Mohd Atan, An estimation of exponential sums associated with a cubic form, *J. Physical Sci.* **10** (1999), 1-21.
[8] S. H. Sapar and K. A. Mohd Atan, Estimate for the Cardinality of the Set of Solution to Congruence Equations (Malay), *J. Technology* No.36(C) (2002), 13–40.