Pertanika 11(1), 125 – 131 (1988)

A Method for Determining the Cardinality of the Set of Solutions to Congruence Equations

KAMEL ARIFFIN MOHD. ATAN
Mathematics Department,
Faculty of Science and Environmental Studies,
Universiti Pertanian Malaysia
43400 Serdang, Selangor, Malaysia

Key words: **Congruence equations; n-tuple polynomials; cardinality; p-adic common zeros.**

ABSTRAK

Kekardinalan set penyelesaian kepada sesuatu sistem persamaan kongruen modulo kuasa perdana, dianggarkan melalui penggunaan kaedah Newton polihedron. Anggaran kepada nilai ini didapatkan bagi n-rangkap polinomial $\underset{\sim}{f} = (f_1, \ldots, f_n)$ *dalam koordinat* $\underset{\sim}{x} = (x_1, \ldots, x_n)$ *dengan pekali dalam* Z_p*. Perbincangan adalah mengenai anggaran yang berkaitan dengan polinomial f yang linear dalam* $\underset{\sim}{x}$ *dan sepasang polinomial yang kuadratik tertentu dalam* $Z_p[x, y]$

ABSTRACT

The cardinality of the set of solutions to a system of congruence equations modulo a prime power is estimated by applying the Newton polyhedral method. Estimates to this value are obtained for an n-tuple of polynomials $\underset{\sim}{f} = (f_1, \ldots, f_n)$ *in coordinates* $\underset{\sim}{x} = (x_1, \ldots, x_n)$ *with coefficients in* Z_p*. The discussion is on the estimates corresponding to the polynomials* $\underset{\sim}{f}$ *that are linear in* $\underset{\sim}{x}$ *and a specific pair of quadratics in* $Z_p[x, y]$*.*

INTRODUCTION

For each prime p and Z_p the ring of p-adic integers let $\underset{\sim}{f} = (f_1 \ldots, f_n)$ be an n-tuple of polynomials in $Z_p[\underset{\sim}{x}]$ where $\underset{\sim}{x} = (x_1, \ldots, x_n)$. We will consider the set

$$V(\underset{\sim}{f}\,; p^\alpha) = \left\{ u \bmod p^\alpha : f(u) \cong O \bmod p^\alpha \right\}$$

where $\alpha > 0$. Let $N(f\,; p^\alpha) = \text{card } V(f\,; p^\alpha)$.

For a polynomial f(x) defined over the ring of integers Z Sandor showed that

$$N(f\,; p^\alpha) \leqslant mp^{\frac{1}{2} \text{ord}_p D}$$

where $D \neq 0$, $\alpha > \text{ord}_p D$ and D is the discriminant of f.

Let K be the algebraic number field generated by the roots ξ_i, $1 \leqslant i \leqslant m$ of the polynomial f(x) with m distinct zeros. Let D(f) denote the different of f the intersection of the fractional ideals of K generated by the numbers

$$\frac{f^{(e_i)}(\xi_i)}{e_i!}$$

$i \geqslant 1$ where e_i is the multiplicity of the root ξ_i.

Loxton and Smith (1982) showed that

$$N(\underset{\sim}{f}\,; p^\alpha) \leqslant mp^{\alpha - (\alpha - \delta)/e}$$

where $\delta = \mathrm{ord}_p D(f)$. With this suitably defined global different of f(x) Loxton and Smith thus improved on the result of Sandor's. Both results are stated for polynomials defined over Z. They, however, can be adapted to work over Z_p.

Chalk and Smith (1982) obtained a result of similar form with $\delta = \max_i \mathrm{ord}_p f_i$ where f_i is the Taylor coefficient $\dfrac{f_i^{(e_i)}(\xi_i)}{e_i!}$ at the distinct roots ξ_i. The proof used a version of Hensel's Lemma.

For $\underset{\sim}{f} = (f_1, \ldots, f_n)$ an n-tuple of polynomials in $Z[\underset{\sim}{x}]$ define the discriminant $D(\underset{\sim}{f})$ of $\underset{\sim}{f}$ as follows. If the resultant of $\underset{\sim}{f}$ and the Jacobian of $\underset{\sim}{f}$ vanishes set $D(\underset{\sim}{f}) = 0$ otherwise let D(f) be the smallest positive integer in the ideal in $Z[\underset{\sim}{x}]$ generated by the Jacobian of $\underset{\sim}{f}$ and the components of $\underset{\sim}{f}$. Loxton and Smith (1982) showed that

$$N(\underset{\sim}{f}, p^\alpha) \leqslant \begin{cases} p^{n\alpha} & \text{for } \alpha \leqslant 2\delta \\ (\mathrm{Deg}\,\underset{\sim}{f})\, p^{n\delta} & \text{for } \alpha > 2\delta \end{cases}$$

where Deg $\underset{\sim}{f}$ means the product of the degrees of all the components of $\underset{\sim}{f}$.

In this paper we will arrive at an estimate of $N(\underset{\sim}{f}\,; p^\alpha)$ for certain polynomials $\underset{\sim}{f}$ by using the Newton polyhedral method as described by Mohd Atan (1986). With p denoting a prime, we define the valuation on Q_p the field of p-adic numbers as usual. That is

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x} & \text{if } x \neq 0 \\ 0 \quad \text{if } x = 0 \end{cases}$$

where $\mathrm{ord}_p x$ denotes the highest power of p dividing x and $\mathrm{ord}_p x = \infty$ if x = 0. The valuation extends uniquely from Q_p to $\overline{Q}_p$ the algebraic closure of Q_p and to Ω_p, and Ω_p is complete and algebraically closed.

2. AN ESTIMATE FOR $N(f\,; p^\alpha)$ WITH f(x) IN Z[x]

In this section we will consider a polynomial f(x) with integer coefficients. Suppose

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = a_0\pi(x - \xi_j)^{e_j}$$

where the ξ_j's are distinct algebraic numbers with respective multiplicities e_j. Let $\delta(f) = \mathrm{ord}_p D(f)$ as before and $e(f) = \max_j \mathrm{ord}_p \dfrac{f_j^{(e_j)}(\xi_j)}{e_j!}$

Then the following theorem gives an estimate for $N(f\,; p^\alpha)$. The proof is a modification of that by Loxton and Smith (1982) illustrating the use of the Newton polygon of f whose special property is stated in Koblitz (1977) which we rewrite as follows.

Lemma 2.1

Let p be a prime and f(x) a polynomial with coefficients in the complete field Ω_p. If a segment of the Newton polygon of f has slope λ, and horizontal length N(i.e. it extends from $(i, \mathrm{ord}_p a_i)$ to $(i + N, \lambda N + \mathrm{ord}_p a_i)$) then f has precisely N root α_i in Ω_p with $\mathrm{ord}_p\, \alpha_i = -\lambda$ (counting multiplicities).

Theorem 2.1

Let p be a prime and f a polynomial with integer coefficients which does not vanish identically modulo p. Set e = e(f), $\delta = \delta(f)$ and let m be the number of distinct zeros of f. Then

$$N(f\,; p^\alpha) \leqslant mp^{\alpha - (\alpha - \delta)/e}$$

Proof:

As above we write

$$f(x) = a_o x^n + a_1 x^{n-1} + \ldots + a_n = a_o \prod_{j=1}^{m} (x - \xi_j)^{e_j}$$

where the ξ_j's are distinct with multiplicities e_j. We may suppose that Ω_p contains the number field K generated by the roots ξ_j. Let $V_j(f\,; p^\alpha)$ denote the set of points in $V(f\,; p^\alpha)$ which are p-adically closest to ξ_j, that is

$$V_j(f\,; p^\alpha) = \left\{ x \text{ in } V(f\,; p^\alpha) : \mathrm{ord}_p(x - \xi_j) = \max_{1 \leqslant i \leqslant m} \mathrm{ord}_p(x - \xi_i)\,. \right\}$$

Then

$$\text{card } V(f\,;p^{\alpha}) \leqslant \sum_{j=1}^{m} \text{card } V_j(f\,;p^{\alpha}).$$

To estimate the terms on the right, we introduce the set

$$D_j(\theta) = \left\{ x \text{ in } \Omega_p : \text{ord}_p(x - \xi_j) = \max_{1 \leqslant i \leqslant m} \text{ord}_p(x - \xi_i) \text{ and } \text{ord}_p f(x) \geqslant \theta \right]$$

and define

$$\gamma_j(\theta) \;=\; \inf_{x \text{ in } D_j(\theta)} \text{ord}_p(x - \xi_j).$$

Since $V_j(f\,;p^{\alpha})$ is a subset of $D_j(\alpha)$, we have

$$\text{card } V_j(f\,;p^{\alpha}) \leqslant \text{card}\left\{ x \bmod p^{\alpha} : \text{ord}_p(x - \xi_j) \geqslant \gamma_j(\alpha) \right] \leqslant p^{\alpha - \gamma_j(\alpha)}$$

We now require a lower bound for $\gamma_j(\alpha)$. For this choose η in $D_j(\theta)$ and consider the Newton polygon of the polynomial $f(x + \eta)$. Let $\mu_j = \text{ord}_p(\eta - \xi_j)$ and let ϵ_j be the total multiplicity of all the roots ξ_j with $\text{ord}_p(\eta - \xi_j) = \mu_j$ and set $\lambda_j = \text{ord}_p \dfrac{f^{(\epsilon_j)}(\xi_j)}{\epsilon_j!}$.

We have

$$\frac{f^{(\epsilon_j)}(\eta)}{\epsilon_j!} = a_o \pi(\eta - \xi_i)^{e_i} + \ldots$$

where $\text{ord}_p(\eta - \xi_i) < \mu_j$ for all i,

and the dots indicate terms with larger p-adic orders than the main term. Thus

$$\text{ord}_p \frac{f^{(\epsilon_j)}(\eta)}{\epsilon_j!} = \lambda_j.$$

In the same way,

$$\text{ord}_p f(\eta) = \lambda_j + \epsilon_j \mu_j \geqslant \theta$$

and for any $k \geqslant 0$

$$\text{ord}_p \frac{f^{(k)}(\eta)}{k!} \geqslant \lambda_j - (i - \epsilon_j)\mu_j.$$

This shows that the first edge of the Newton polygon of $f(x + \eta)$ goes from the point $(0, \text{ord}_p f(\eta))$ to the point $(\epsilon_j, \text{ord}_p \dfrac{f^{(\epsilon_j)}(\eta)}{\epsilon_j!}$ as required by

Lemma 2.1. We can find η so that $\text{ord}_p f(\eta) = \theta$ and $\mu_j = \gamma_j(\theta)$ and for this choice of η we have

$$\gamma_j(\theta) = (\theta - \lambda_j)/\epsilon_j.$$

Therefore $\gamma_j(\theta)$ is continuous, increasing and concave away from the origin. Further if θ is sufficiently large, ξ_j is the unique closest root to η and so $\epsilon_j = e_j$ and

$$\lambda_j = \text{ord}_p \frac{f^{(e_j)}(\xi_j)}{e_j!} = \delta_j \quad \text{(say).}$$

By considering the graph of $\gamma_j(\theta)$ we see that

$$\gamma_j(\theta) \geqslant (\theta - \delta_j)e_j \geqslant (\theta - \delta)/e$$

for $\theta \geqslant \delta$.

Finally,

$$\text{card } V(f\,;p^{\alpha}) \leqslant \max_{1 \leqslant j \leqslant m} \text{card } V_j(f\,;p^{\alpha})$$

$$\leqslant m\, p^{\alpha - (\alpha - \delta)/e}$$

for $\alpha \geqslant \delta$.

This proves the theorem since the required estimate is trivial when $\alpha > \delta$.

3 ESTIMATE FOR $N(\underset{\sim}{f}\,;p^{\alpha})$ WITH $\underset{\sim}{f}(\underset{\sim}{x})$ IN $Z_p[\underset{\sim}{x}]$

In this section we will consider the set

$$V(\underset{\sim}{f}\,;p^{\alpha}) = \left\{ \underset{\sim}{x} \bmod p^{\alpha} : \underset{\sim}{f}(\underset{\sim}{x}) \equiv \underset{\sim}{0} \bmod p^{\alpha} \right\}$$

where $\underset{\sim}{f} = (f_1, \ldots, f_n)$ is an n-tuple of polynomials in the coordinates $\underset{\sim}{x} = (x_1, \ldots, x_n)$ with coefficients in Z_p. We will consider first polynomials f_i, $i = 1, 2, \ldots, n$ that are linear in $(x_1, \ldots, x_n)$ as in the following theorem.

Theorem 3.1

Let p be a prime and $f = (\underset{\sim}{f}_1, \ldots, f_n)$ be an n-tuple of non-constant linear polynomials in $Z_p[\underset{\sim}{x}]$ where $\underset{\sim}{x} = (x_1, \ldots, x_n)$. Suppose r is the rank of matrix A representing $\underset{\sim}{f}$. Let δ be the minimum of the p-adic orders of r x r non-singular submatrices of A. If $\alpha > 0$ then

$$N(\underset{\sim}{f}\,; p^\alpha) \leqslant \begin{cases} p^{n\alpha} & \text{if } \alpha \leqslant \delta \\ p^{(n-r)\alpha + r\delta} & \text{if } \alpha > \delta \end{cases}$$

Proof:

The assertion is trivial for $\alpha \leqslant \delta$. Suppose $\alpha > \delta$. Consider the set

$$V(\underset{\sim}{f}\,; p^\alpha) = \left\{ \underset{\sim}{u} \bmod p^\alpha : \underset{\sim}{f}(\underset{\sim}{u}) \cong O \bmod p^\alpha \right\}$$

The equation

$$\underset{\sim}{f}(\underset{\sim}{x}) \equiv \underset{\sim}{O} \bmod p^\alpha \qquad (1)$$

is equivalent to

$$A\,\underset{\sim}{x} \equiv \underset{\sim}{O} \bmod p^\alpha \qquad (2)$$

where A is the matrix representing f. Now A is equivalent to a matrix A' of the form

$$A' = \begin{bmatrix} B & C \\ O & O \end{bmatrix}$$

where B is an r x r non-singular matrix and C and r x(n−r) matrix both with rational entries. Therefore (2) is equivalent to

$$A'\,\underset{\sim}{x} \equiv \underset{\sim}{O} \bmod p^\alpha \qquad (3)$$

Write $\underset{\sim}{x} = (\underset{\sim}{x}', \underset{\sim}{x}'')^t$ where $\underset{\sim}{x}'$ comprises the first r components of $\underset{\sim}{x}$ and $\underset{\sim}{x}''$ the remainder, and $(a, b)^t$ denotes the transpose of (a, b). Then (3) becomes

$$B\,\underset{\sim}{x}' \equiv -C\,\underset{\sim}{x}'' \bmod p^\alpha \qquad (4)$$

On multiplying both sides of the congruence (4) by the adjoint of B, we obtain

$$(\det B)\underset{\sim}{x}' \equiv -(\operatorname{adj} B)C\,\underset{\sim}{x}'' \bmod p^\alpha \qquad (5)$$

For a given $\underset{\sim}{x}''$ in (5) the number of solutions for $\underset{\sim}{x}' \bmod p^\alpha$ is either o or $p^{r\delta}$ since (5) determines $\underset{\sim}{x}' \bmod p^{\alpha-\delta}$. Thus there are $p^{(n-r)\alpha}$ choices for $\underset{\sim}{x}'' \bmod p^\alpha$. It follows that the number of solutions $\underset{\sim}{x} \bmod p^\alpha$ to (2) and hence (1) is $p^{(n-r)\alpha + r\delta}$ as asserted.

In Theorem 3.1 if $n = 2$, $\alpha > \delta$ and rank $A = 2$ then

$$N(f_1, f_2, p^\alpha) \leqslant p^{2\delta}$$

where δ is the p-adic order of the Jacobian of f_1 and f_2. We will give an alternative proof of this assertion using the Newton polyhedral method. First we have the following lemma.

Lemma 3.1

Let p be a prime and f, g linear functions in the coordinates $\underset{\sim}{x} = (x, y)$ defined over Z_p. Let $J = f_x g_y - f_y g_x$ be their Jacobian. Suppose $\underset{\sim}{x}_o$ in Ω_p^2 statisfies $\operatorname{ord}_p f(\underset{\sim}{x}_o) \geqslant \alpha$ and $\operatorname{ord}_p g(\underset{\sim}{x}_o) \geqslant \alpha$. If $\alpha > \operatorname{ord}_p J$ then f and g have a common zero $\underset{\sim}{\xi}$ in Ω_p^2 with $\operatorname{ordp}(\underset{\sim}{\xi} - \underset{\sim}{x}_o) \geqslant \alpha - \operatorname{ord}_p J$.

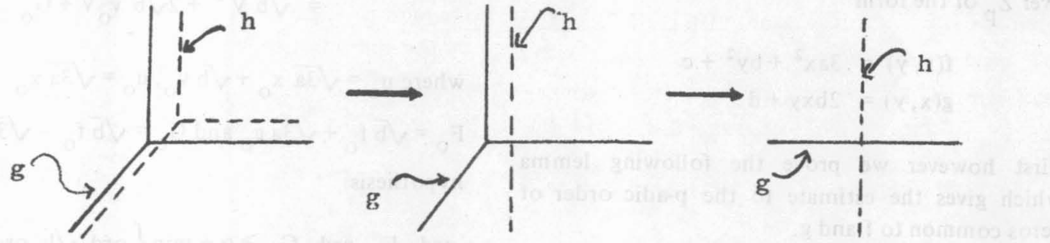
Proof:

Let $X = (\underset{\sim}{X}, Y) = \underset{\sim}{x} - \underset{\sim}{x}_o$ and write

$$f(\underset{\sim}{X} + \underset{\sim}{x}_o) = f_o + f_x X + f_y Y$$
$$g(\underset{\sim}{X} + \underset{\sim}{x}_o) = g_o + g_x X + g_y Y$$

where $f_o = f(\underset{\sim}{x}_o)$, $g_o(\underset{\sim}{x}_o)$.

Consider the indicator diagrams (as defined by Mohd Atan (1986)) of $f(\underset{\sim}{X}) + \underset{\sim}{x}_o)$ and $g(\underset{\sim}{X} + \underset{\sim}{x}_o)$. If no edges in these diagrams coincide, then by Mohd Atan (1986) there exists a zero common to f and g statisfying $\operatorname{ord}_p X \geqslant \alpha - \operatorname{ord}_p J$. If some edges coincide but with say $\operatorname{ord}_p f_o/f_x \leqslant \operatorname{ord}_p g_o/g_x$ we replace g by $g - (g_y/f_y)f$ to eliminate Y. This transformation does not change J and the hypothesis of the lemma are satisfied with the



same α as before. If no edges of the indicator diagrams coincide we can apply the same result by Mohd Atan (1986) above to get the desired conclusion. Otherwise we replace f by $f - (f_x/g_x)g$ to eliminate X. Again this does not change J and the result is therefore clear. Possible stages in the proof are shown in the following diagrams.

Note:

The above equations can be obtained at once by solving the simultaneous equations $f(\underset{\sim}{X} + \underset{\sim}{x}_o) = g(\underset{\sim}{X} + \underset{\sim}{x}_o) = 0$ for $\underset{\sim}{X}$. It is to avoid solving the equations and to illustrate the use of Newton polyhedron that we consider the above result.

The following theorem gives an alternative proof using Newton polyhedral method to Theorem 3.1 when $n = 2$, $\alpha > \delta$ and rank of matrix representing f_1, f_2 is equal to 2.

Theorem 3.2

Let f and g be linear polynomials in $Z_p[x, y]$. Let $J_{f,g}$ be the Jacobian of f and g and $\delta = \text{ord}_p J_{f,g}$, Let $\alpha > 0$. Then

$$N(f\,;g\,;p^{\alpha}) \leqslant \begin{cases} p^{2\alpha} & \text{if } \alpha \leqslant \delta \\ p^{2\delta} & \text{if } \alpha > \delta \end{cases}$$

Proof: The result is trivial for $\alpha \leqslant \delta$. We assume next $\alpha > \delta$. As before let

$$V(f\,;g\,;p^{\alpha}) = \left\{ (x, y) \bmod p^{\alpha} : f(x, y),\ g(x, y) \equiv 0 \bmod p^{\alpha} \right\}.$$

Consider the set

$$H(\lambda) = \left\{ (x, y) \text{ in } \Omega_p^2 : \text{ord}_p f(x, y),\ \text{ord}_p g(x, y) \geqslant \lambda \right\}$$

for any real number λ. Define

$$\gamma(\lambda) = \inf_{\underset{\sim}{x} \in H(\lambda)} \text{ord}_p (\underset{\sim}{x} - \underset{\sim}{\xi})$$

where $\underset{\sim}{x} = (x, y)$ and $\underset{\sim}{\xi}$ is the common zero of f and g.

$$V(f; g; p^{\alpha}) \subseteq H(\alpha)$$

for each $\alpha \geqslant 1$, it follows that

$$\text{card } V(f; g; p^{\alpha}) \leqslant \text{card}\left\{ \underset{\sim}{x} \bmod p^{\alpha} : \text{ord}_p (\underset{\sim}{x} - \underset{\sim}{\xi}) \geqslant (\alpha) \right\} \leqslant p^{2\alpha - 2\gamma(\alpha)} \qquad (1)$$

where $\alpha \geqslant \gamma(\alpha)$.

The lower bound for the function $\gamma : R \to R$ can be found by examining the indicator diagrams associated with the Newton polynomials of $f(X + \underset{\sim}{x}_o)$ and $g(\underset{\sim}{X} + \underset{\sim}{x}_o)$ for $\underset{\sim}{x}_o$ in $H(\lambda)$. By our hypothesis and Lemma 3.1,

$$\gamma(\alpha) \geqslant \alpha - \delta$$

It follows by (1) that

$$\text{card } V(f; g; p^{\alpha}) \leqslant p^{2\delta}$$

Since $\text{ord}_p J_{f,g} < \infty$, f and g have a unique common zero. Hence

$$N(f; g; p^{\alpha}) \leqslant p^{2\delta}$$

as required.

Next, we will consider a pair of non-linear polynomials f and g in coordinates (x, y) defined over Z_p of the form

$$f(x, y) = 3ax^2 + by^2 + c$$
$$g(x, y) = 2bxy + d.$$

First however we prove the following lemma which gives the estimate to the p-adic order of zeros common to f and g.

Lemma 3.2

Let $f(x, y) = 3ax^2 + by^2 + c$, $g(x, y) = 2bxy + d$ be polynomials with coefficients in Z_p and with $p > 2$. Let $\delta = \max\left\{\mathrm{ord}_p 3a, \frac{3}{2}\,\mathrm{ord}_p b\right\}$ Suppose (x_o, y_o) is in Ω_p^2 with

$$\mathrm{ord}_p\, f(x_o, y_o), \mathrm{ord}_p\, g(x_o, y_o) \geqslant \alpha > \delta.$$

Then, there is a point (ξ, η) in Ω_p^2 with $f(\xi, \eta) = g(\xi, \eta) = 0$ and $\mathrm{ord}_p\,(\xi - x_o), \mathrm{ord}_p(\eta - y_o) \geqslant \frac{1}{2}(\alpha - \delta)$

Proof:

Write $\underset{\sim}{X} = (X, Y) = \underset{\sim}{x} - \underset{\sim}{x}_o$ and set

$$f(X, Y) = 3aX^2 + bY^2 + 6ax_oX + 2by_oY + f_o$$

$$g(X, Y) = 2bXY + 2by_oX + 2bx_oY + g_o$$

where

$$f_o = 3ax_o + by_o{}^2 + c$$

$$g_o = 2bx_oy_o + d.$$

With the change of variable

$$U = \sqrt{3a}\,X + \sqrt{b}\,Y$$
$$V = \sqrt{3a}\,X - \sqrt{b}\,Y$$

we find that

$$F(U, V) = \sqrt{b}\, f(X, Y) + \sqrt{3a}\, g(X, Y)$$
$$= \sqrt{b}\, U^2 + 2\sqrt{b}\, u_oU + F_o$$

and

$$G(U, V) = \sqrt{b}\, f(X, Y) + \sqrt{3a}\, g(X, Y)$$
$$= \sqrt{b}\, V^2 + 2\sqrt{b}\, v_oV + G_o$$

where $u_o = \sqrt{3a}\,x_o + \sqrt{b}\,y_o$, $u_o = \sqrt{3a}\,x_o - \sqrt{b}\,y_o$, $F_o = \sqrt{b}\,f_o + \sqrt{3a}\,g_o$ and $G_o = \sqrt{b}\,f_o - \sqrt{3a}\,g_o$. By hypothesis

$$\mathrm{ord}_p\, F_o, \mathrm{ord}_p\, G_o \geqslant \alpha + \min\left\{\mathrm{ord}_p\sqrt{b}, \mathrm{ord}_p\sqrt{3a}\right\}$$

We therefore see from the Newton polygon of F, that F has a zero satisfying

$$\mathrm{ord}_p\, U \geqslant \frac{1}{2}\,\mathrm{ord}_p\,\frac{F_o}{\sqrt{b}} \geqslant \frac{1}{2}\,\alpha + \min\left\{0, \mathrm{ord}_p\sqrt{3a/b}\right\}$$

A similar result holds for G. These estimates lead to a zero (X, Y) of f and g satisfying the required inequality.

The following theorem gives the estimate for $N(f; g; p^\alpha)$ where f and g are quadratics in the above form.

Theorem 3.3

Let $f(x, y) = 3ax^2 + by^2 + c$ and $g(x, y) = 2bxy + b$ be polynomials with coefficients in Z_p where p is a prime > 2. Let $\alpha > 0$ and

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

Then

$$N(f; g; p^\alpha) \leqslant \begin{cases} p^{2\alpha} & \text{if } \alpha \leqslant \delta \\ 4p^{\alpha + \delta} & \text{if } \alpha > \delta \end{cases}$$

Proof:

We consider the case when $\alpha > \delta$. The result is trivial when $\alpha \leqslant \delta$. As before let

$$V(f; g; p^\alpha) = \left\{(x, y) \bmod p^\alpha : f(x, y), g(x, y) \equiv 0 \bmod p^\alpha\right\}$$

Following the method of Loxton and Smith (1982) we take $V_i(f; g; p^\alpha)$ to indicate the set of points in $V(f; g; p^\alpha)$ that are p-adically close to a common zero $\underset{\sim}{\xi}_i = (\xi_{i1}, \xi_{i2})$ of f and g. That is

$$V_i(f; g; p^\alpha) = \left\{\underset{\sim}{x} \in V(f; g; p^\alpha) : \mathrm{ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_i) = \max_j \mathrm{ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_j)\right\}$$

where $\underset{\sim}{x} = (x, y)$. Then

$$N(f; g; p^{\alpha}) \leqslant \sum_i \text{card } V_i(f; g; p^{\alpha}) \quad (1)$$

Consider the set

$$H_i'(\lambda) = \{\underset{\sim}{x} \in \Omega_p^2 ; \text{ ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_i) = \max \text{ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_j) \text{ and } \text{ord}_p f(x), \text{ord}_p g(\underset{\sim}{x}) \geqslant \lambda\}$$

For any real number λ. Define

$$\gamma_i(\lambda) = \inf_{\underset{\sim}{x} \in H_i(\lambda)} \text{ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_i)$$

for all i. Now, for every $\alpha \geqslant 1$.

$$V_i(f; g; p^{\alpha}) \subseteq H_i(\alpha).$$

It follows that

$$\text{card } V_i(f; g; p^{\alpha}) \leqslant \text{card}\{\underset{\sim}{x} \bmod p^{\alpha} : \text{ord}_p(\underset{\sim}{x} - \underset{\sim}{\xi}_i) \geqslant \gamma_i(\alpha)\} \leqslant p^{2\alpha - 2\gamma_i(\alpha)} \quad (2)$$

where $\alpha \geqslant \gamma_i(\alpha)$ for all i.

We find the lower bound for the function $\gamma_i : R \rightarrow R$ by examining the combination of the indicator diagrams for $f(\underset{\sim}{X} + \underset{\sim}{x}_o)$ and $g(\underset{\sim}{X} + \underset{\sim}{x}_o)$ with (x_o, y_o) in $H_i(\lambda)$. By hypothesis and Lemma 3.2

$$\gamma_i(\alpha) \geqslant \frac{1}{2}(\alpha - \delta).$$

Hence, by (2)

$$\text{card } V_i(f; g; p^{\alpha}) \leqslant p^{\alpha + \delta} \quad (3)$$

for all i. By a theorem of Bezout (see for example Hartshorne (1977) or Shafarevich (1977) the number of common zeros of $f(\underset{\sim}{X} + \underset{\sim}{x}_o)$ and $g(X + \underset{\sim}{x}_o)$ does not exceed the product of the degrees of f and g. Hence by (1) and (3) the above assertion holds.

CONCLUSION

In this paper we give estimates for $N(\underset{\sim}{f}, p^{\alpha})$ where $\underset{\sim}{f} = (f_1, \ldots, f_n)$ is an n-tuple polynomials in the coordinates $\underset{\sim}{x} = (x_1, \ldots, x_n)$ and coefficients in Z_p. We have considered both linear polynomials and a pair of non-linear polynomials of a specific form. Our discussion is centred in the use of Newton polyhedral method to arrive at these estimates. The extension to a more general method to arrive at the estimates for $N(f, p^{\alpha})$ where $\underset{\sim}{f} = (f_1, \ldots, f_n)$ are n-tuple of non-linear polynomials of a more general form will be the subject of our next discussion.

ACKNOWLEDGEMENT

The author would like to express his gratitude to Professor J.H. Loxton of the University of Macquarie of Australia for suggesting the problem and for enlightening discussions leading to the results.

REFERENCES

KOBLITZ, N. (1977): "p-adic power series" p-adic Numbers, p-adic Analysis and Zeta-Functions, Springer-Verlag New York, Berlin, 1977.

CHALK, J.H.H. and R.A. SMITH (1982): Sandor's Theorem On Polynomial Congruences and Hensel's Lemma C.R. *Math. Rep. Acad. Sci. Canada* **4(1):**

HARTSHORNE, R. (1977): Algebraic Geometry Springer Verlag, New York, Berlin, 53–54.

LOXTON, J.H. and R.A. SMITH, (1982): On Hua's estimate for exponential sums. *J. London Math. Soc.* **26(2):** 15–20.

LOXTON, J.H. and R.A. SMITH (1982): On Hua's esti-Exponential Sums. *J. Australian Math. Soc.* **33:** 125–134.

MOHD ATAN, K.A. (1986): Newton Polyhedra and p-adic Estimates of Zeros of Polynomials in $\Omega_p[x, y]$" *Pertaniaka* **9(1):** 51–56. Universiti Pertanian Malaysia.

MOHD ATAN, K.A. (1986): Newton Polyhedral Method of Determining p-adic Orders of Zeros Common to Two Polynomials in $Q_p[x, y]$. *Pertanika* **9(3).** 375–380. Universiti Pertanian Malaysia.

SHAFAREVICH, I.R. (1977): Basic Algebraic Geometry Springer Verlag, Berlin, New York, 198.

(Received 30 November, 1987)