Pertanika J. Sci. & Technol. **1(2)**:249-260 (1993)

ISSN: 0128-7680

On the Estimate to Solutions of Congruence Equations Associated with a Cubic Form

Kamel Ariffin Mohd. Atan[1] and Ismail bin Abdullah[2]

[1]Department of Mathematics
[2]Department of Computer Science
Faculty of Science and Environmental Studies,
Universiti Pertanian Malaysia,
43400 UPM Serdang, Selangor Darul Ehsan, Malaysia

Received 23 November 1992

ABSTRAK

Set penyelesaian kepada persamaan kongruen kuasa perdana yang disekutukan dengan polinomial

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

dalam $Z_p[x,y]$ diperiksa dan kekardinalannya dianggar dengan menggunakan teknik polihedron Newton. Kaedah ini melibatkan penurunan persamaan pembezaan separa bagi f kepada polinomial satu pembolehubah dan mencari δ, faktor penentu dalam anggaran di atas. f_x dan f_y diturunkan menjadi polinomial satu pembolehubah dengan menggunakan parameter-parameter yang sesuai. Polihedron Newton yang disekutukan dengan polinomial yang diperolehi dipertimbangkan. Terdapat pensifar-pensifar sepunya bagi polinomial-polinomial satu pembolehubah dengan peringkat p-adic yang bersesuaian dengan titik persilangan dalam gabungan gambarajah-gambarajah penunjuk yang disekutukan dengan polihedron Newton masing-masing. Ini menghasilkan saiz pensifar-pensifar sepunya bagi pembezaan separa bagi f. Maklumat ini digunakan bagi mendapatkan anggaran di atas.

ABSTRACT

The set of solutions to congruence equations modulo a prime power associated with the polynomial

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

in $Z_p[x,y]$ is examined and its cardinality estimated by employing the Newton polyhedral technique. The method involves reduction of the partial derivatives of f to single-variable polynomials and finding δ the determinant factor in the estimation. f_x and f_y are reduced to one-variable polynomials by the employment of suitable parameters. The Newton polyhedrons associated with the polynomials so obtained are then considered. There exist common zeros of the single-variable polynomials whose p-adic orders correspond to the intersection points in the combination of the indicator diagrams associated with the respective Newton polyhedrons. This leads to sizes of common zeros of the partial derivatives of f. This information is then used to arrive at the above estimate.

Keywords: **congruence equations, p-adic orders, Newton polyhedron method, indicator diagrams.**

INTRODUCTION

Let p be a prime, and let $\underline{f} = (f_1, \ldots, f_n)$ be an n-tuple of polynomials in $\underline{x} = (x_1, \ldots, x_n)$ with coefficients in the p-adic ring Z_p. Denote by $N(\underline{f}\ ; p^\alpha)$ the cardinality of the set

$$V(\underline{f}; p^\alpha) = \{\underline{u} \bmod p^\alpha \ : \underline{f}(\underline{u}) \equiv \underline{0} \bmod p^\alpha\}$$

where $\alpha > 0$ and each component of $\underline{u}$ runs through a complete set of residues modulo p^α. To find the estimates of $N(\underline{f}\ ; p^\alpha)$ has been the subject of research of many authors, such as in the work to find the best possible estimates to multiple exponential sums associated with each $\underline{f}$.

Loxton and Smith (1982a), for example, showed that for $\alpha > 0$.

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

if $\alpha > \delta$, where m is the number of distinct roots of $f(x) \in Z[x]$ that generate its associated algebraic number field K, and δ is the highest power of p dividing D(f), where D(f) denotes the intersections of the fractional ideals of K generated by the number $\frac{f^{(e_i)}(\xi_i)}{e_i!}$, $1 \leq i$ and $e = m_iaxe_i$ where e_i is the multiplicity of ξ_i.

Chalk and Smith (1982) obtained a similar result by using a version of Hensel's Lemma. Loxton and Smith (1982b) showed that for $\underline{f} = (f_1, \ldots, f_n)$.

$$N(\underline{f}\ ; p^\alpha) \leqslant \begin{cases} p^{n\alpha} & \text{for } \alpha \leqslant 2\delta \\ (\text{Deg } \underline{f})\ p^{n\delta} & \text{for } \alpha > 2\delta \end{cases}$$

where $\delta = \text{ord}_p \Delta(\underline{f})$ and $\Delta(\underline{f})$ denotes the discriminant of $\underline{f}$. Mohd Atan (1988) considered linear polynomials $\underline{f}$ with coefficients in the p-adic ring Z_p and showed that

$$N(\underline{f}\ ; p^\alpha) \leqslant \min\{p^{n\alpha}, p^{(n-r)\alpha + r\delta}\}$$

where δ indicates the minimum of the p-adic orders of r x r non-singular submatrices of the reduced coefficient matrix of $\underline{f}$. The author also considered in particular the non-linear polynomial $\underline{f} = (f_x, f_y)$ where f_x, f_y are the usual partial derivatives with respect to x and y respectively of the polynomial

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

in $Z_p[x, y]$ and gave the estimate for $N(f_x, f_y, p^\alpha)$ explicitly in terms of the p-adic orders of the coefficients of f(x, y) as follows:

$$N(f_x, f_y; p^\alpha) \leqslant \begin{cases} p^{2\alpha} \text{ if } \alpha \leqslant \delta \\ 4p^{\alpha+\delta} \text{ if } \alpha > \delta \end{cases}$$

where $\delta = \max\{\operatorname{ord}_p 3a, 3/2 \operatorname{ord}_p b\}$.

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 a result of similar form with $\delta = \max\{\operatorname{ord}_p 3a, \operatorname{ord}_p b\}$ which then generalises slightly the former.

In this paper we will consider the same cubic form as in Mohd Atan and Abdullah (1992). We will show that δ is in fact the p-adic order of at least one of the coefficients of the dominant terms of the cubic form. We will employ the Newton polyhedral method as described by Mohd Atan (1986) in our discussion. With p denoting a prime, we define the valuation on Q_p the field of p-adic number as usual. That is,

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

where $\operatorname{ord}_p x$ denotes the highest power of p dividing x and $\operatorname{ord}_p x = \infty$, if x = 0. $||_p$ extends uniquely from Q_p to $\overline{Q}_p$ the algebraic closure of Q_p and to Ω_p the completion of the algebraic closure of Q_p.

P-ADIC SIZES OF COMMON ZEROS

Mohd Atan and Loxton (1986) introduced the p-adic Newton polyhedral method for finding the p-adic properties of zeros of polynomials in $\Omega_p[x, y]$. Mohd Atan (1986) applied this method to investigate the p-adic properties of common zeros of two polynomials by considering the combinations of the indicator diagrams associated with the Newton polyhedrons of both. He conjectured that to every simple point of intersection of the combination there exist common zeros of both polynomials whose p-adic orders correspond to this point. He then proved a special case of the conjecture which we rewrite as follows.

Theorem 2.1

Let p be a prime. Suppose f and g are polynomials in $Z_p[x,y]$. Let (λ, μ) be a point of intersection of the indicator diagrams associated with f and g which is not a vertex of either diagram and suppose that the edges through (λ, μ) do not coincide. Then there are ξ and η in Ω_p satisfying $f(\xi,\eta) = g(\xi,\eta) = 0$ and $\mathrm{ord}_p\xi = \lambda$, $\mathrm{ord}_p\eta = \mu$.

Mohd Atan (1988) considered polynomials of the form

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

whose partial derivatives with respect to x and y, respectively are

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

in $Z_p[x, y]$. By applying Theorem 2.1, he showed that if for some (x_0, y_0) in $\Omega^2_{p.}$

$$\mathrm{ord}_p f(x_0, y_0), \mathrm{ord}_p\, g(x_0, y_0) \geqslant \alpha > \delta$$

where > 0 and $\delta = \max\{\mathrm{ord}_p 3a, 3/2\ \mathrm{ord}_p b\}$, then there is a point (ξ,η) in Ω^2_p at which f and g vanishes and $\mathrm{ord}_p(\xi - x_0)$, $\mathrm{ord}_p(\eta - y_0) \geqslant 1/2(\alpha - \delta)$.

Mohd Atan and Abdullah (1992) considered the polynomials $h = f_x$, $g = f_y$ where f_x and f_y denote the partial derivatives with respect to x and y respectively of the more general polynomial

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

with (x_0, y_0) and α as above. They obtained a similar result as above, with

$$\delta = \max\{\mathrm{ord}_p 3a, \mathrm{ord}_p b\}.$$

We will now consider the polynomial $h = f_x$ and $g = f_y$, where f(x,y) is as immediately above, and show that δ is in fact the p-adic order of at least one of the coefficients of the dominant terms of f(x,y). Our assertion is as in the following theorem which improves a similar assertion in Theorem 2.2 of the above-mentioned paper.

Theorem 2.2

Let $f(x,y) = 3ax^2 + 2bxy + cy^2 + k$ and $g(x,y) = bx^2 + 2cxy + 3dy^2 + m$ be polynomials in $Z_p[x,y]$. Let $\alpha > 0$ and

$$\delta = \max\{\text{ord}_p 3a, \text{ord}_p b, \text{ord}_p c, \text{ord}_p 3d\}$$

Suppose (x_0, y_0) is in Ω^2_p with

$$\text{ord}_p f(x_0, y_0), \text{ord}_p g(x_0, y_0) \geqslant \alpha > \delta$$

Then there is a point (ξ, η) in Ω^2_p with $f(\xi, \eta) = g(\xi, \eta) = 0$ and $\text{ord}_p(\xi - x_0)$, $\text{ord}_p(\eta - y_0) > 1/2(\alpha - \delta)$.

Proof:

Let $X = x - x_{0;}$ $Y = y - y_0$. Then,

$$f(X,Y) = 3aX^2 + 2bXY + cY^2 + f_x X + f_y Y + f_0$$
$$g(X,Y) = bX^2 + 2cXY + 3dY^2 + g_x X + g_y Y + g_0$$

where h_z denotes the partial derivative of h with respect to z defined at (x_0, y_0) and $h_0 = h(x_0, y_0)$.

Let α, β be the zeros of

$$u(x) = (c^2 - 3bd)x^2 + (bc - 9ad)x + (b^2 - 3ac)$$

If $\alpha \neq \beta$ then as in Mohd Atan and Abdullah (1992), the polynomials

$$F(U,V) = (3a + b\alpha)(f + \alpha g)$$
$$G(U,V) = (3a + b\beta)(f + \beta g)$$

where

$$U = (3a + b\alpha)X + (b + c\alpha)Y$$
$$V = (3a + b\beta)X + (b + c\beta)Y$$

will have a simple intersection in their combined indicator diagrams associated with their respective Newton polyhedrons. By Theorem 2.1, they showed eventually that there is a common zero (ξ, η) of f and g with

$$\mathrm{ord}_p(\xi - x_0),\ \mathrm{ord}_p(\eta - y_0 \geqslant \frac{1}{2}\ (\alpha - \delta_0\ )$$

where $\delta_0 = \max\ \{\mathrm{ord}_p 3\alpha,\ \mathrm{ord}_p b\ \}$.

It is possible that U or V as defined above could attain the zero value. Under such circumstances we exchange the roles of the variables X and Y since the result will be symmetrical in X and Y. Hence this would always ensure that U and V are non-zero.

Clearly, from our hypothesis,

$$\mathrm{ord}_p x_0\,,\ \mathrm{ord}_p y_0\ \ \geqslant \frac{1}{2}\ (\alpha - \delta\ )$$

since $\delta_0 \leqslant \delta$.

Suppose now $\alpha = \beta$.

Consider the linear combination of f and g as follows

$$\begin{aligned} G(X,Y) &= (3a + b\alpha)^2\ (cf - bg) \\ &= (3ac - b^2)(3a + b\alpha)^2\ X^2 - (3bd - c^2\ )(3a + b\alpha\ )^2\ Y^2 \\ &+ (3a + b\alpha)^2\ [c\ f_x - b\ g_x\ )\ X + (c\ f_y - b\ g_y\ )\ Y\ ] \\ &+ (3a + b\alpha)^2\ (cf_0 - b\ g_0) \end{aligned} \qquad (1)$$

Since α is a double root of u(x),we have $\alpha^2 = \dfrac{b^2 - 3ac}{c^2 - 3bd}$ and $(bc - 9ad)^2$ $= 4(b^2 - 3ac)(c^2 - 3bd)$. Thus we have

$$(3bd - c^2)(3a + b\alpha)^2 = (3ac - b^2)(b + c\alpha\ )^2$$

Hence (1) becomes

$$\begin{aligned} G(X,Y) &= (3ac - b^2)\{(3a\ + b\alpha)^2\ X^2 - (b + c\alpha)^2\ Y^2\ \} \\ &+ (3a + b\alpha)^2\ [cf_x - bg_x\ )X + (cf_y - bg_y\ )Y\ ] \\ &+ (3a + b\alpha)^2\ (cf_0 - bg_0) \end{aligned} \qquad (2)$$

Let

$$\begin{aligned} U &= (3a + b\alpha)X + (b + c\alpha)Y \\ V &= (3a + b\alpha)X - (b + c\alpha)\ Y \end{aligned} \qquad (3)$$

Now, since

$$f_x = 6ax_0 + 2by_0,$$
$$f_y = g_x = 2bx_0 + 2cy_0,$$
$$g_y = 2cx_0 + 6dy_0,$$

by (3), (2) will become

$$\begin{aligned} G(U,V) &= (b^2 - 3ac)UV + (b^2 - 3ac)[(3a + b\alpha)x_0 - (b + c\alpha)y_0]U \\ &+ (b^2 - 3ac)[(3a + b\alpha)x_0 + (b + c\alpha)y_0]V \\ &+ (3a + b\alpha)^2(cf_0 - bg_0) \end{aligned} \tag{4}$$

Similarly, with F as in the beginning of the proof and substitution of (3), we have

$$F(U,V) = U^2 + 2[(3a + b\alpha)x_0 + (b + c\alpha)y_0]U + (3a + b\alpha)(f_0 + \alpha g_0) \tag{5}$$

Rewrite (4) and (5) as follows

$$F(U,V) = U^2 + AU + (3a + b\alpha)(f_0 + \alpha g_0) \tag{6}$$

$$G(U,V) = BUV + CU + DV + (3a + b\alpha)^2(cf_0 - bg_0) \tag{7}$$

where

$$\begin{aligned} A &= 2[(3a + b\alpha)x_0 + (b + c\alpha)y_0] \\ B &= (b^2 - 3ac) \\ C &= (b^2 - 3ac)[(3a + b\alpha)x_0 - (b + c\alpha)y_0] \\ D &= (b^2 - 3ac)[(3a + b\alpha)x_0 + (b + c\alpha)y_0] \end{aligned}$$

Then (6) and (7) can be rewritten as

$$\begin{aligned} F(T,W) &= T^2 - (3a + b\alpha)(f_0 + \alpha g_0) \\ G(T,W) &= TW \end{aligned}$$

where

$$W = BV + C \tag{8}$$
$$T = U + D / B \tag{9}$$

Consider the indicator diagrams associated with the Newton polyhedrons of F(T,W) and G(T,W). They are of the shape as shown in *Fig. 1.*

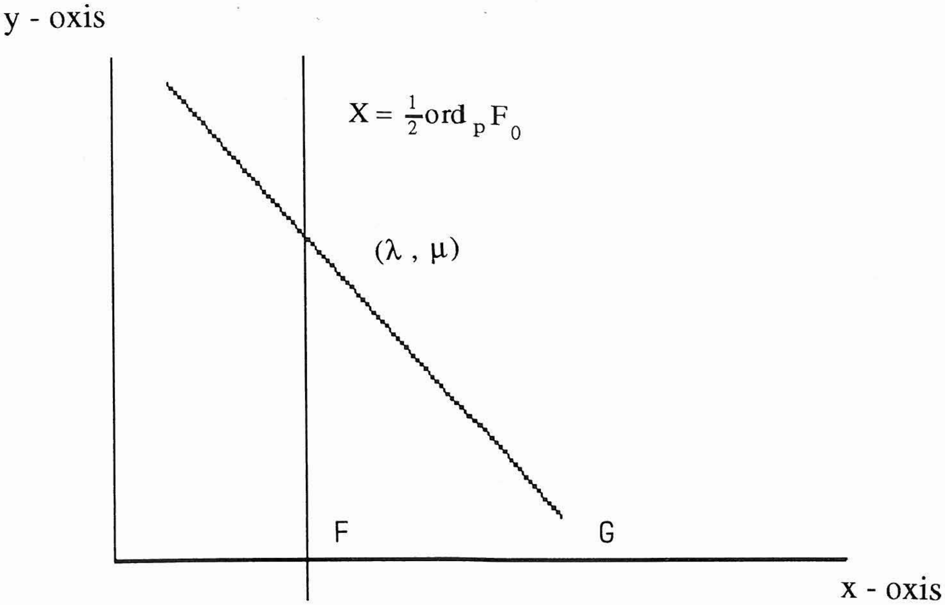

Fig. 1. The combined indicator diagrams associated with F and G

Clearly, the indicator diagrams of F and G will have a simple intersection point at the point $\left(\frac{1}{2}\text{ord}_p(3a + b\alpha)(f_0 + \alpha g_0),\infty\right)$.

By Theorem 1.1 of Mohd Atan (1986) there exists (T_0, W_0) in Ω_p^2 such that $F(T_0,W_0) = G(T_0,W_0) = 0$ and

$$\text{ord}_p T_0 = \frac{1}{2}\ \text{ord}_p\ (3a + b\alpha)(f_0 + g_0) \tag{10}$$

$$\text{ord}_p W_0 = \infty$$

By definition, $W_0 = 0$. Thus by (8),(9), there exists (U_0,V_0) with

$$U_0 = T_0 - \frac{D}{B} \tag{11}$$

$$V_0 = -\frac{C}{B} \tag{12}$$

Now, by (3), there exists X_0, Y_0 such that

$$X_0 = \frac{U_0 + V_0}{2(3a + b\alpha)}$$

$$Y_0 = \frac{U_0 - V_0}{2(b + \alpha c)}$$

By (10),(11),(12) and definitions of B, C and D we will have

$$\mathrm{ord}_p X_0 \geqslant \frac{1}{2}\,[\mathrm{ord}_p(f_0 + \alpha g_0) - \mathrm{ord}_p(3a + b\alpha)]$$

or

$$\mathrm{ord}_p X_0 \geqslant \frac{1}{2}\,[\alpha - \delta]$$

and

$$\mathrm{ord}_p Y_0 \geqslant \frac{1}{2}\,[\mathrm{ord}_p(f_0 + \alpha g_0) - \mathrm{ord}_p(\ c + 3d\alpha)]$$

or

$$\mathrm{ord}_p Y_0 \geqslant \frac{1}{2}\,[\alpha - \delta]$$

The existence of X_0 and Y_0 and their p-adic estimates will lead to a common zero $(\xi\ , \eta\ )$ of f and g with $X_0 = \xi - x_0$, $Y_0 = \eta - y_0$ and the required estimate.

ESTIMATION OF $N(f_x, f_y, p^\alpha)$

Let p be a prime as usual, and f_x, f_y the partial derivatives of a polynomial f. Mohd Atan (1988) showed that for the polynomial $f(x, y) = ax^3 + bxy^2 + cx + dy + e$ in $Z_p\,[x,y]$,

$$N(f_x, f_y\ ; p^\alpha) \leqslant \min\{p^{2\alpha}, 4p^{\alpha+\delta}\}$$

where $\delta = \max\{\mathrm{ord}_p 3a, \frac{3}{2}\ \mathrm{ord}_p b\}$.

We will obtain an estimate for $N(f_x, f_y\ ; p^\alpha)$ of similar form associated with the polynomial

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

in Z_p [x,y] as follows.

Theorem 3.1

Let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + kx + my + n$ be a polynomial in $Z_p[x,y]$

Let $\alpha > 0$ and $\delta = \max \{\mathrm{ord}_p 3a, \mathrm{ord}_p b, \mathrm{ord}_p c, \mathrm{ord}_p 3d\}$.

Then,

$$N(f_x , f_y ; p^\alpha) \leqslant \begin{cases} p^{2\alpha} \text{ if } \alpha \leqslant \delta \\ 4p^{\alpha+\delta} \text{ if } \alpha > \delta \end{cases}$$

Proof:

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

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

Let

$$V_i (f_x, f_y ; p^\alpha) = \{ \underline{x} \in V(f_x; f_y ; p^\alpha):\mathrm{ord}_p(\underline{x} - \underline{\xi}_i) = \max_j \mathrm{ord}_p(\underline{x} - \underline{\xi}_j)\}$$

where $\underline{x}$ = (x, y) and $\underline{\xi}_i$ is a common zero of f_x and f_y.

Consider the set

$$H_i(\lambda) = \left\{ \underline{x} \varepsilon \Omega_p^2 : \mathrm{ord}_p(\underline{x} - \underline{\xi}_i) = \max_j \mathrm{ord}_p(\underline{x} - \underline{\xi}_j) \wedge \mathrm{ord}_p f_x(\underline{x}), \mathrm{ord}_p f_y(\underline{x}) \geq \lambda \right\}$$

for any real number λ. Next, define

$$\gamma_i(\lambda) = \inf_{\underline{x} \in H_i(\lambda)} \mathrm{ord}_p(\underline{x} - \underline{\xi}_i)$$

for all i. Loxton and Smith (1982a) showed that

$$N_i(f_x; f_y; p^\alpha) \leqslant p^{2\alpha - 2\gamma_i(\alpha)} \tag{13}$$

where $\alpha \geqslant \gamma_i(\alpha)$ for all i and $N_i(f_x ; f_y ; p^\alpha)$ indicates the cardinality of $V_i(f_x;f_y;p^\alpha)$. We find the lower bound for the function γ_i: R → R by examining the combined indicator diagrams of $f_x(\underline{X} + \underline{x}_0)$ and $f_y(\underline{X} + \underline{x}_0)$ with (x_0, y_0) in $H_i(\alpha)$. By hypothesis and Theorem 2.1

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

Hence by (13)

$$N_i(f_x ; f_y ; p\alpha) \leqslant p^{\alpha+\delta} \tag{14}$$

for all i.

In non-degenerate cases the polynomials $f_x(\underline{X} + \underline{x}_0)$ and $f_y(\underline{X} + \underline{x}_0)$ have a finite number of common zeros. In these cases, by a theorem of Bezout (see for example Hartshorne (1977)) the number of common zeros of both polynomials does not exceed the product of the degrees of f_x dan $f_{y.}$ Also, it is clear that

$$N(f_x;f_y;p^\alpha) \leq \sum_i N_i(f_x;f_y;p^\alpha)$$

Hence by (14) the above assertion holds.

However in the generate cases where the polynomials have infinitely many common roots the above argument breaks down. This will be the subject of further investigation.

CONCLUSION

The result for $N(f_x ; f_y ; p^\alpha)$ obtained above for the polynomial of Theorem 3.1 is for the polynomial considered by Mohd Atan and Abdullah (1992). In our case we have shown that the value of the determining factor δ is in fact dependent on the dominant terms of f. This gives a more symmetric result than the previous one. In both cases the method is to first reduce both polynomials f_x , f_y to polynomials in one variable and next consider combination of the indicator diagrams associated with the p-adic Newton polyhedrons of each polynomial. Reduction of both polynomials to one-variable polynomials requires finding suitable parameters that can be employed in the linear combinations of both to yield the one-variable polynomial so desired. The reduction process is continuously carried out until a combination of indicator diagrams with a simple intersection is obtained. This point is examined further to arrive eventually at our result.

REFERENCES

CHALK, J. H. H. and R. A. SMITH. 1982. Sandor's theorem on polynomials congruences and Hensel's Lemma. *C.R. Math. Rep. Acad. Sci., Canada* **4(1):** 49-54.

HARTSHORNE, R. 1977. *Algebraic Geometry*. New York: Springer Verlag. 53-54.

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

LOXTON, J. H. and R. A. SMITH. 1982b. Estimates for multiple exponential sums. *J. Aust. Math. Soc.* **33:** 125-134.

MOHD. ATAN, K. A. 1986. Newton polyhedral method of determining p-adic orders of zeros common to two polynomials in Q [x,y]. *Pertanika* **9(3):** 375-380.

MOHD. ATAN, K. A. 1988. A method for determining the cardinality of the sets of solutions to congruence equations. *Pertanika* **11(1)**: 125-131.

MOHD. ATAN, K. A. and I. B. ABDULLAH. 1992. Set of solutions to congruence equations associated with a cubic form. *Journal of Physical Science* **3:** 1-6.

MOHD. ATAN, K. A. and J.H. LOXTON. 1986. Newton polyhedra and solutions of congruences. *Diophantine Analysis, LMS* **109:** 67-82.