
Conference collection
International Conference
on Mathematics, Engineering
and Industrial Applications 2018
(ICoMEIA2018)
Proceedings of the 2nd International
Conference on Mathematics, Engineering
and Industrial Applications 2018
AIP Conference Proceedings

MENU SIGN IN/REGISTER

ORDER PRINT EDITION
AIP Conference Proceedings
The 18th International Conference on Positron Annihilation

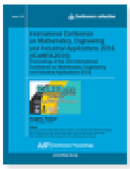
AIP Conference Proceedings

HOME BROWSE MORE

Table of Contents

INTERNATIONAL CONFERENCE ON MATHEMATICS, ENGINEERING AND INDUSTRIAL APPLICATIONS 2016 (ICoMEIA2016): Proceedings of the 2nd International Conference on Mathematics, Engineering and Industrial Applications 2016

PREV NEXT



Conference date: 10–12 August 2016
Location: Songkhla, Thailand
ISBN: 978-0-7354-1433-4
Editors: Nursalasawati Rusli, Wan Mohd Khairy Adly Wan Zaimi, Khairul Anwar Mohamad Khazali, Maz Jamilah Masnan, Wan Suhana Wan Daud, Nooraihan Abdullah, Zainab Yahya, Nor Azrita Mohd Amin, Nurul Huda Abdul Aziz and Yusmye Nur Abu Yusuf
Volume number: 1775
Published: Oct 24, 2016

DISPLAY : 20 50 100 all

BROWSE VOLUMES

MENU SIGN IN/REGISTER

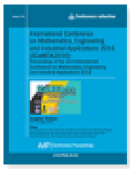
AIP Conference Proceedings

HOME BROWSE MORE

Table of Contents

INTERNATIONAL CONFERENCE ON MATHEMATICS, ENGINEERING AND INDUSTRIAL APPLICATIONS 2016 (ICoMEIA2016): Proceedings of the 2nd International Conference on Mathematics, Engineering and Industrial Applications 2016

< PREV NEXT >



Conference date: 10–12 August 2016
Location: Songkhla, Thailand
ISBN: 978-0-7354-1433-4
Editors: Nursalasawati Rusli, Wan Mohd Khairy Adly Wan Zaimi, Khairul Anwar Mohamad Khazali, Maz Jamilah Masnan, Wan Suhana Wan Daud, Nooraihan Abdullah, Zainab Yahya, Nor Azrita Mohd Amin, Nurul Huda Abdul Aziz and Yusmye Nur Abu Yusuf
Volume number: 1775
Published: Oct 24, 2016

DISPLAY : 20 50 100 all

BROWSE VOLUMES

PRELIMINARY

No Access . October 2016

Preface: International Conference on Mathematics, Engineering and Industrial Applications 2016

AIP Conference Proceedings **1775**, 010001 (2016); https://doi.org/10.1063/1.4965119

KEYNOTE PAPER

No Access . October 2016

The current scenario of industrial mathematics in Malaysia

Zainal Abdul Aziz and Arifah Bahar

AIP Conference Proceedings **1775**, 020001 (2016); https://doi.org/10.1063/1.4965120

SHOW ABSTRACT

CONTRIBUTED ORAL PAPERS

No Access . October 2016

On some properties of an epidemiological delay integral equation

Manuel De la Sen

AIP Conference Proceedings **1775**, 030001 (2016); https://doi.org/10.1063/1.4965121

SHOW ABSTRACT

BROWSE VOLUMES

On the symbolic manipulation for the cardinality of certain degree polynomials

Ismail Abdullah, Kamaruzzaman Seman, Bachok M. Taib and Fitri Maya Puspita

AIP Conference Proceedings **1775**, 030051 (2016); https://doi.org/10.1063/1.4965171

SHOW ABSTRACT

No Access . October 2016

Analysis of parameters' effects in semi-automated knee cartilage segmentation model: Data from the osteoarthritis initiative

Hong-Seng Gan, Ahmad Helmy Abdul Karim, Khairil Amir Sayuti, Tian-Swee Tan and Mohammed Rafiq Abdul Kadir

AIP Conference Proceedings **1775**, 030052 (2016); https://doi.org/10.1063/1.4965172

SHOW ABSTRACT

No Access . October 2016

A review on the statistical concepts of six sigma

Faisal Ali and Amran Ahmed

AIP Conference Proceedings **1775**, 030053 (2016); https://doi.org/10.1063/1.4965173

SHOW ABSTRACT

No Access . October 2016

An efficient rice yield predictive model in lower northern Thailand

BROWSE VOLUMES

AIP Conference Proceedings **1775**, 030097 (2016); https://doi.org/10.1063/1.4965217

SHOW ABSTRACT

No Access . October 2016

Semi-implicit method for solving one dimensional shallow water equation

Siti Maryam Hafiza Mohd Kanafiah and Nursalasawati Rusli

AIP Conference Proceedings **1775**, 030098 (2016); https://doi.org/10.1063/1.4965218

SHOW ABSTRACT

1 2 >

ABOUT

CONTACT

HELP

PRIVACY POLICY

TERMS OF USE

FOLLOW AIP PUBLISHING:

Scitation

BROWSE VOLUMES


SUMMER SALE!
AIP Conference Proceedings
30% OFF
ALL PRINT PROCEEDINGS!
ENTER COUPON CODE SUMMER2017

On the Symbolic Manipulation for the Cardinality of Certain Degree Polynomials

Ismail Abdullah[1,a)], Kamaruzzaman Seman[1,b)], Bachok M. Taib[1,c)] and Fitri Maya Puspita[2, d)]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM)*
71800 Bandar Baru Nilai, Negeri Sembilan, Malaysia
[2]*Mathematics Department, Faculty of Mathematics and Natural Sciences, University of Sriwijaya*
Inderlaya, Ogan Ilir, South Sumatra, Indonesia

[a)]Corresponding author: isbah@usim.edu.my
[b)]drkzaman@usim.edu.my
[c)]bachok@usim.edu.my
[d)]fitrimayapuspita@unsri.ac.id

Abstract. The research on cardinality of polynomials was started by Mohd Atan [1] when he considered a set, $V(\underline{f};p^\alpha)=\{u \bmod p^\alpha : \underline{f}(u)\cong 0 \bmod p^\alpha\}$, where $\alpha>0$ and $\underline{f}=(f_1,f_2,...,f_n)$. The term $\underline{f}(u)\cong \underline{0} \bmod p^\alpha$ means that we are considering all congruence equations of modulo p^α and we are looking for u that makes the congruence equation equals zero. This is called the zeros of polynomials. The total numbers of such zeros is termed as $N(\underline{f};p^\alpha)$. The above p is a prime number and Z_p is the ring of p-adic integers, and $\underline{x}=(x_1,x_2,...,x_n)$. He later let $N(\underline{f};p^\alpha)=\text{card } V(\underline{f};p^\alpha)$. The notation $N(\underline{f};p^\alpha)$ means the number of zeros for that the polynomials $\underline{f}$. For a polynomial $f(x)$ defined over the ring of integers Z, Sandor [2] showed that $N(f;p^\alpha)\le mp^{\frac{1}{2} ord_p D}$, where $D\neq 0, \alpha > ord_p D$ and D is the discriminant of f. In this paper we will try to introduce the concept of symbolic manipulation to ease the process of transformation from two-variables polynomials to one-variable polynomials.

INTRODUCTION

The research on cardinality of polynomials was started by [1] when he considered a set,

$$V(f;p^\alpha)=\{u \bmod p^\alpha : f(u)\cong 0 \bmod p^\alpha\} \tag{1}$$

where $\alpha>0$ and $\underline{f}=(f_1,f_2,...,f_n)$. The term $f(u)\cong 0 \bmod p^\alpha$ means that we are considering all congruence equations of modulo p^α and determine u that makes the congruence equation equals zero. This is called the zeros of polynomials. The total numbers of such zeros is termed as $N(\underline{f};p^\alpha)$.

The above p is a prime number and Z_P is the ring of p-adic integers, and $\underline{x}=(x_1,x_2,...,x_n)$. He later let $N(\underline{f};p^\alpha)=\text{card } V(\underline{f};p^\alpha)$. The notation $N(\underline{f};p^\alpha)$ means the number of zeros for that the polynomials $\underline{f}$.

International Conference on Mathematics, Engineering and Industrial Applications 2016 (ICoMEIA2016)
AIP Conf. Proc. 1775, 030051-1–030051-7; doi: 10.1063/1.4965171
Published by AIP Publishing. 978-0-7354-1433-4/$30.00

For a polynomial $f(x)$ defined over the ring of integers Z, Sandor [2] showed that

$$N(f;p^{\alpha}) \le mp^{\frac{1}{2}ord_p D} \tag{2}$$

Where $D \neq 0, \alpha > ord_p D$ and D is the discriminant of f.

The following is a further explanation of how [1] arrived at his first result in this research. Let K be the algebraic number field generated by the roots $\xi_i, 1 \le i \le m$ of the polynomials $f(x)$ with m distinct zeros. Let $D(f)$ denotes the different of f the intersection of the fractional ideals of K generated by the numbers, $\frac{f^{(e_i)}(\xi_i)}{e_i!}$, $i \ge 1$ where e_i is the multiplicity of the roots ξ_i.

The authors [3] showed that

$$N(f;p^{\alpha}) \le mp^{\alpha-(\alpha-\delta)/e} \tag{3}$$

where $\delta = ord_p D(f)$, with this suitably defined global different of $f(x)$ Loxton and Smith [3] thus improved on the result of Sandor's. Both results are stated for polynomials defined over Z. They, however can be adopted to work over Z_p.

Chalk and Smith [4] obtained a result of similar form with $\delta = \max_i ord_p f_i$ where f_i is the Taylor coefficient $f^{(e_i)}(\xi_i)/e_i!$ at the distinct roots ξ_i. The proof used a version of Hensel's Lemma.

For $\underline{f} = (f_1, f_2, ..., f_n)$ an n-tuple of polynomials in $Z[\underline{x}]$ define the discriminant $D(\underline{f})$ of $\underline{f}$ as follows. If the resultant of $\underline{f}$ and the Jacobian of $\underline{f}$ vanishes set $D(\underline{f}) = 0$ otherwise let $D(\underline{f})$ be the smallest positive integer in the ideal in $Z[\underline{x}]$ generated by the Jacobian of $\underline{f}$ and the components of $\underline{f}$. The authors [3] showed that

$$N(\underline{f};p^{\alpha}) \le \begin{cases} p^{n\alpha}, & \text{for } \alpha \le 2\delta \\ (\text{Deg } \underline{f})p^{n\delta}, & \text{for } \alpha > 2\delta \end{cases} \tag{4}$$

Where $(\deg \underline{f})$ means the product of the degrees of all the components of $\underline{f}$.

In his work [1] for certain polynomials using Newton polyhedral method as described by [5] had arrived at an estimate of $N(f;p^{\alpha})$. He proposed a valuation on Q_P the field of p-adic numbers as

$$|x|_p \le \begin{cases} p^{-ord_p x}, \text{if } x \neq 0 \\ 0, \quad \text{if } x = 0 \end{cases} \tag{5}$$

This valuation extends uniquely from Q_P to $\bar{Q}_P$ the algebraic closure of Q_P and to Ω_P, and Ω_P is complete and algebraically closed.

ESTIMATE FOR $N(\underline{f};p^{\alpha})$ WITH $\underline{f}(x)$ IN $Z[\underline{x}]$

Let us consider a polynomial $f(x)$ with integer coefficient such as

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

where ξ_j are distinct algebraic numbers with respective multiplicities e_j. Let $\delta(f) = ord_p D(f)$ as before and $e(f) = \max_j ord_p \left\{ \frac{f^{(e_j)}(\xi_j)}{e_j!} \right\}$. Then the following theorem gives an estimate for $N(f;p^\alpha)$. The proof is a modification of that by [3] illustrating the use of the Newton polygon of f whose special property is stated in [6] which [1] rewrite as follows

Lemma 1. Let p be a prime and $f(x)$ be 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 extending from $(i, ord_p a_i)$ to $(i+N, \lambda N + ord_p a_i)$ is N then f has precisely N roots α_i in Ω_P with $ord_p \alpha_i = -\lambda$ (counting multiplicities).

Theorem 1. Let p be a prime and $f(x)$ be a polynomial with 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

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

Proof. As above we write,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = a_0 \prod_{j=1}^{m} (x-\xi_j)^{e_j}$$

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

$$V_j(f;p^\alpha) = \left\{ x \in V(f;p^\alpha) = ord_p(x-\xi_i) = \max_{1\le i\le m} ord_p(x-\xi_i) \right\}$$

Then,

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

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

$$D_j(\theta) = \left\{ x \in \Omega_p : ord_p(x-\xi_i) = \max_{1\le i\le m} ord_p(x-\xi_i) \,\&\, ord_p f(x) \ge \theta \right\}$$

and define $\gamma_j(\theta) = \inf_{x\in D_j(\theta)} ord_p(x-\xi_j)$. Since $V_j(f;p^\alpha) \subseteq D_j(\alpha)$, we have card $V_j(f;p^\alpha) \le card \left\{ x \bmod p^\alpha : ord_p(x-\xi_i) \ge \gamma_j(\alpha) \right\} \le p^{\alpha-\gamma_j(\alpha)}$. We now need a lower bound for $\gamma_j(\alpha)$. For this, choose $\eta \in D_j(\theta)$ and consider the Newton polygon of the polynomial $f(x+\eta)$. Let $\mu_j = ord_p(\eta-\xi_j)$ and let ε_j be the total multiplicity of all the roots ξ_j with $ord_p(\eta-\xi_j) = \mu_j$ and set $\lambda_j = ord_p \, f^{(\varepsilon_j)}(\xi_j) / \varepsilon_j!$. We have

$$\frac{f^{(\varepsilon_j)}(\eta)}{\varepsilon_j!} = a_0 \prod (\eta-\xi_i)^{e_i} + \ldots.$$

where $ord_p(\eta-\xi_i) < \mu_j, \forall i$, and the dots indicate terms with larger p-adic orders than the main term. Thus $ord_p \frac{f^{(\varepsilon_j)}(\eta)}{\varepsilon_j!} = \lambda_j$. In the same way, $ord_p f(\eta) = \lambda_j + \varepsilon_j \mu_j \ge \theta$ and for any $k \ge 0$, $ord_p \frac{f^{(k)}(\eta)}{k!} \ge \lambda_j - (i-\varepsilon_j)\mu_j$. This shows that the first edge of the Newton polygon of $f(x+\eta)$ goes from the point $(0, ord_p f(\eta))$ to the point

$(\varepsilon_j, ord_p \frac{f^{(\varepsilon_j)}(\eta)}{\varepsilon_j!})$ as required by Lemma 2. We can find η so that $ord_p f(\eta) = \theta$, $\mu_j = \gamma_j(\theta)$ and for this choice of η we have $\gamma_j(\theta) = (\theta - \lambda_j)/\varepsilon_j$. 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 $\varepsilon_j = e_j$ and, $\lambda_j = ord_p \frac{f^{(e_j)}(\xi_j)}{e_j!} = \delta_j$ (say). By considering the graph of $\gamma_j(\theta)$ we see that $\gamma_j(\theta) \geq (\theta - \delta_j)e_j \geq (\theta - \delta)/e$ for $\theta \geq \delta$. Finally, card $V(f;p^\alpha) \leq \max_{1\leq j\leq m}$ card $V_j(f;p^\alpha) \leq mp^{\alpha-(\alpha-\delta)/e}$, for all $\alpha \geq \delta$. This proves the theorem since the required estimate is trivial when $\alpha \geq \delta$.

Let us consider further the set $V(f;p^\alpha) = \{x \bmod p^\alpha : f(x) \equiv 0 \bmod p^\alpha\}$ where $\underline{f} = (f_1,...,f_n)$ is an n-tuple of polynomials in the coordinate $\underline{x} = (x_1,...,x_n)$ with coefficients in Z_p. We will consider first polynomials $f_i, i = 1,2,...,n$ that are linear in $(x_1,...,x_n)$ as in the following theorem:

Theorem 2. Let p be a prime and $\underline{f} = (f_1,...,f_n)$ be an n-tuple of non-constant linear polynomials in $Z_p[\underline{x}]$ where $\underline{x} = (x_1,...,x_n)$. Suppose r is the rank of matrix A representing $\underline{f}$. Let δ be the minimum of the p-adic orders of $r \times r$ non-singular submatrices of A if $\alpha > 0$ then

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

Proof. The result is trivial if $\alpha \leq \delta$. Suppose $\alpha > \delta$. Consider the set, $V(\underline{f};p^\alpha) = \{\underline{u} \bmod p^\alpha : \underline{f}(\underline{u}) \cong 0 \bmod p^\alpha\}$.

The equation,

$$\underline{f}(\underline{x}) \cong \underline{0} \bmod p^\alpha \tag{6}$$

is equivalent to

$$A\underline{x} \cong \underline{0} \bmod p^\alpha \tag{7}$$

where A matrix representing f. Now A is equivalent to a matrix A' of the form, $A' = \begin{bmatrix} B & C \\ 0 & 0 \end{bmatrix}$, where B is an $r \times r$ non-singular matrix and C is an $r \times (n-r)$ matrix both with rational entries. Therefore (7) is equivalent

$$A'\underline{x} \cong \underline{0} \bmod p^\alpha \tag{8}$$

Write $\underline{x} = (\underline{x}', \underline{x}'')^t$, where $\underline{x}'$ comprises the first r components of $\underline{x}$ and $\underline{x}''$ the remainder, and $(a,b)^t$ denotes the transpose of (a,b). Then (8) becomes,

$$B\underline{x}' \equiv -C\underline{x}'' \bmod p^\alpha \tag{9}$$

On multiplying both sides of the congruence (9) by the adjoint of B, we obtain

$$(\det B)\underline{x}' \equiv -(\text{adj } B)C\underline{x}'' \bmod p^\alpha \tag{10}$$

For a given $\underline{x}''$ in (10) the number of solutions for $\underline{x}' \bmod p^\alpha$ is either 0 or $p^{r\delta}$ since (10) determines $\underline{x}' \bmod p^{\alpha-\delta}$. Thus there are $p^{(n-r)\alpha}$ choices for $\underline{x}'' \bmod p^\alpha$. It follows that the number of solutions $\underline{x} \bmod p^\alpha$ to (7) and hence (6) is $p^{(n-r)\alpha+r\delta}$ as claimed. In theorem 2, if $n = 2, \alpha > \delta$ and rank $A = 2$ then $N(f_1, f_2, p^\alpha) \leq p^{2\delta}$, where δ is the p-adic order of the Jacobian of f_1 and f_2. We will give an alternative proof of this claim using the Newton polyhedral method. First we have the following lemma.

Lemma 2. Let p be a prime and f,g linear functions in the coordinate $\underline{x}=(x,y)$ define over Z_p. Let $J=f_x g_y - f_y g_x$ be their Jacobian. Suppose x_0 in Ω_p^2 satisfies $ord_p f(\underline{x}_0)\geq\alpha$ and $ord_p g(\underline{x}_0)\geq\alpha$. If $\alpha > ord_p J$ then f and g have common zeros $\underline{\xi}$ in Ω_p^2 with $ord_p(\underline{\xi}-\underline{x}_0)\geq\alpha - ord_p J$.

Proof.

Let $X=(\underline{X},Y)=\underline{x}-\underline{x}_0$ and write

$f(\underline{X}+\underline{x}_0)=f_0+f_x X+f_y Y$

$g(\underline{X}+\underline{x}_0)=g_0+g_x X+g_y Y$

where $f_0=(f(\underline{x}_0),g(\underline{x}_o))$.

Consider the indicator diagrams [7] of $f(\underline{X}+\underline{x}_0)$ and $g(\underline{X}+\underline{x}_0)$. If no edges in these diagrams coincide, then by Mohd Atan [5] there exists a zero common to f and g satisfying $ord_p X\geq\alpha-ord_p J$. If some edges coincide but with say $ord_p\left({f_0}/{f_x}\right)\leq ord_p\left({g_0}/{g_x}\right)$ we replace g by $g-\left({g_y}/{f_y}\right)f$ 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 diagram coincides we can apply the same result [7] above to get the desired conclusion. Otherwise we replace f by $f-\left({f_x}/{g_x}\right)g$ 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 $f(\underline{X}+\underline{x}_0)=g(\underline{X}+\underline{x}_0)=0$ for $\underline{X}$. It is to avoid solving the equations and to illustrate the use of Newton polyhedrons that we consider the above result.

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

Theorem 2. Let f and g be two linear polynomials in $Z_p[x,y]$. Let $J_{f,g}$ be the Jacobian of f and g and $\delta=ord_p J_{f,g}$. Let $\alpha>0$. Then

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

Proof. The result is trivial for $\alpha\leq\delta$. 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,

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

For any real λ. Define, $\gamma(\lambda)=\inf_{\underline{x}\in H(\lambda)} ord_p(\underline{x}-\underline{\xi})$, where $\underline{x}=(x,y)$ and $\underline{\xi}$ is the common zeros of f and g.

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

For each $\alpha \geq 1$, it follows that

$$\text{card}\, V(f;g;p^{\alpha}) \leq card\left\{\underline{x} \bmod p^{\alpha} : ord_p(x-\xi) \geq \alpha\right\} \leq p^{2\alpha - 2\theta(\alpha)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(11)$$

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

The lower bound for the function $\gamma : R \rightarrow R$ can be found by examining the indicator diagrams associated with the Newton polyhedrons of $f(X+\underline{x}_0)$ and $g(X+\underline{x}_0)$ for $\underline{x}_0$ in $H(\lambda)$. By our hypothesis and Lemma 2, $\gamma(\alpha) > \alpha - \delta$. It follows by (3) that, $\text{card}\, V(f;g;p^{\alpha}) \leq p^{2\delta}$. Since $ord_p J_{f,g} < \infty$, f and g have a unique common zero. Hence $N(f;g;p^{\alpha}) \leq p^{2\delta}$ as required. As seen from [1], he used Newton polyhedron technique. In that technique he introduced a device called Indicator Diagram to locate the common zeros of two polynomials. Each polynomial will produce one indicator diagram. The two indicator diagrams belonging to two polynomials will be drawn on the same space to see whether there is coincidence on the sides or not. If there exists coincidence, then a transformation process to one variable polynomial will be used to come up with a clear intersection.

SYMBOLIC MANIPULATION

The author would like to call this as Newton Polyhedron Technique and subsequently this method will be used by other researchers later. The following steps will elaborate the sequences of manipulations that can be applied to solve the problem of reducing two-variables polynomial to one-variable polynomial and thus N. Koblitz's method can be applied to find the estimates.

Step 1 : The two polynomials

Consider two non-linear polynomials as follows:

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

Step 2 : the transformation process

Let $\underline{X} = (X,Y) = \underline{x} - \underline{x}_0$ and set;

$f(X,Y) = 3aX^2 + bY^2 + 6ax_0X + 2by_0Y + f_0$ and $g(X,Y) = 2bXY + 2by_0X + 2bx_0Y + g_0$

where, $f_0 = 3ax_0{}^2 + by_0{}^2 + c$ and $g_0 = 2bx_0y_0 + d$.

Step 3 : The symbolic Manipulations

With the change of variables, $U = \sqrt{3a}X + \sqrt{b}Y$ and $V = \sqrt{3a}X - \sqrt{b}Y$, we will find that

$F(U,V) = \sqrt{b}f(X,Y) + \sqrt{3a}g(X,Y) = \sqrt{b}U^2 + \sqrt{3a}u_0U + F_0$ and

$G(U,V) = \sqrt{b}f(X,Y) + \sqrt{3a}g(X,Y) = \sqrt{b}V^2 + \sqrt{3a}v_0V + G_0$

where,

$u_0 = \sqrt{3a}x_0 + \sqrt{b}y_0$ and $v_0 = \sqrt{3a}x_0 - \sqrt{b}y_0$

$F_0 = \sqrt{b}f_0 + \sqrt{3a}g_0$ and $G_0 = \sqrt{b}f_0 - \sqrt{3a}g_0$

Step 4 : Deriving the conclusion

By hypothesis,

$$ord_p F_0, ord_p G_0 \geq \alpha + \min\left\{ord_p \sqrt{b}, ord_p \sqrt{3a}\right\}$$

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

$$ord_p U \geq \frac{1}{2} ord_p \frac{F_0}{\sqrt{b}} \geq \frac{1}{2}\left[\alpha + \min\left\{0, ord_p \sqrt{\frac{3a}{b}}\right\}\right]$$

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

Step 5 : Stating the estimates

Mohd Atan [1] arrived at the estimates as shown below. He started with two polynomials of an incomplete cubic form, i.e. $f(x,y) = 3ax^2 + by^2 + c$ and $g(x,y) = 2bxy + d$. He has done the steps 1 until 4 and obtaining $\delta = \max\left\{ord_p 3a, \frac{3}{2} ord_p b\right\}$ and the estimate as

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

CONCLUSION

Symbolic manipulation seems to be crucial for this research to move further as it will later involve higher degree of polynomials. The use of Computer Algebra System MAXIMA will be looked into carefully to help us in transforming two-variables polynomials to one-variable polynomials. In one-variable polynomial the monumental work of Koblitz can be applied to determine the cardinality of polynomials.

ACKNOWLEDGEMENT

This research is partially supported by FRGS research grant USIM/FRGS/FST/32/50214.

REFERENCES

1. Mohd Atan, K. A. A. Pertanika **11**(1), 125 – 131, 1988.
2. Sandor, J., Borislav, C., Handbook of Number Theory II, 2004.
3. Loxton, J. H. and R. A. Smith. J. London Math. Soc. **26**(2): 15 – 20, 1982.
4. Chalk, J.H.H. and R.A.Smith. Math. Rep. Acad. Sci. Canada, **4**(1), 1982.
5. Mohd Atan, K. A. Pertanika **9**(1): 51 – 56, 1986.
6. Koblitz, N. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics No. 58, Springer-Verlag, New York, 1977.
7. Mohd Atan, K. A. Pertanika **9**(3): 375 – 380, 1986.