UNIVERSITI PUTRA MALAYSIA

ON THE ESTIMATE TO SOLUTIONS OF CONGRUENCE EQUATIONS ASSOCIATED WITH A QUARTIC FORM

CHAN KAIT LOON

FSAS 1997 6

ON THE ESTIMATE TO SOLUTIONS OF CONGRUENCE EQUATIONS ASSOCIATED WITH A QUARTIC FORM

BY

CHAN KAIT LOON

Thesis Submitted in Fulfilment of the Requirements
for the degree of Master of Science in the
Faculty of Science and Environmental Studies
Universiti Putra Malaysia
April 1997

ACKNOWLEDGEMENTS

I would like to express my most gratitude and sincere appreciation to my chairman Prof. Dr. Kamel Ariffin bin Mohd. Atan and Dr. Ismail Abdullah for their untiring guidance, valuable advice, support and comments. Their patience and persistent encouragement during the course of my research is instrumental to the completion of this thesis.

I also wish to thank the Head of Department, Assoc. Prof. Dr. Harun Budin, academic and general staff of the Department of Mathematics, Universiti Putra Malaysia, for their assistance in various capacities.

Last but not least, I would like to thank my family and friends for their understanding, support and encouragement throughout the course of this study.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

p	Prime Number
α	Exponent of Prime Numbers
Z	Ring of Integers
Q	Field of Rational Numbers
R	Field of Real Numbers
C	Field of Complex Numbers
Ω_p	Completion of $\overline{Q}_p$
$\underline{x}$	n Tuple of Variable $(x_1,\ldots,x_n)$
F	Ring or Field
$F[\underline{x}]$	Ring of Polynomials with Coefficients in F
$\underline{f}$	n Tuple of Polynomials $(f_1$
$Deg(\underline{f})$	Degree of $\underline{f}$
$ord_p\, a$	Highest Power of p which Divides a
$\nabla \underline{f}$	Gradient of $\underline{f}$
N_f	Newton Polyhedron of f
V	Vertex of N_f
E	Edge of N_f
L	Projection of N_f

δ	Determinant Factor
max	Maximum
min	Minimum
mod	Modulo
Exp	Exponential
$\vert\,\vert_p$	Valuation respect to p
$\sum$	Summation
det A	Determinant A
(a,b)	Greatest Common Divisor of a and b

Abstract of thesis submitted to the Senate of Universiti Putra Malaysia in fulfilment of the requirements for the degree of Master of Science.

ON THE ESTIMATE TO SOLUTIONS OF CONGRUENCE EQUATIONS ASSOCIATED WITH A QUARTIC FORM

By

CHAN KAIT LOON

APRIL 1997

Chairman : Professor Dr. Kamel Ariffin bin Mohd. Atan

Faculty : Science and Environmental Studies

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

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 + mx + ny + k$$

in $Z_p[x,y]$ is examined and its cardinality is estimated by employing the Newton polyhedral technique.

The method involves reduction of the partial derivatives of f that is f_x and f_y into polynomials with single variable and finding δ the determinant factor in the estimation. f_x and f_y are reduced to one-variable polynomials by employment of suitable parameters. The Newton polyhedrons associated with the polynomials so obtained are then considered and combination of their Indicator diagrams examined.

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 of the polynomials. The p-adic sizes of these zeros are then determined, and this leads to sizes of common zeros of the partial derivatives of f. This information is then used to arrive at the estimate of the cardinality above.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi syarat bagi Ijazah Master Sains.

PENGANGGARAN KEPADA PENYELESAIAN BAGI PERSAMAAN KONGRUEN BERSEKUTU DENGAN SATU BENTUK KUARTIK

Oleh

CHAN KAIT LOON

APRIL 1997

Pengerusi : Professor Dr. Kamel Ariffin bin Mohd. Atan

Fakulti : Sains dan Pengajian Alam Sekitar

Penganggaran kekardinalan kepada set penyelesaian bagi persamaan kongruen modulo suatu kuasa perdana yang disekutukan dengan polinomial

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 + mx + ny + k$$

dalam $Z_p [x,y]$ ditentukan dengan menggunakan teknik polihedron Newton.

Kaedah ini meliputi penurunan terbitan separa bagi f iaitu f_x and f_y kepada polinomial satu pembolehubah, kemudian faktor penentu δ bagi anggaran di atas diperolehi. Dalam proses penurunan f_x and f_y, parameter-parameter yang sesuai digunakan. Kemudian polihedron Newton yang disekutukan dengan polinomial satu pembolehubah dipertimbangkan.

Terdapat pensifar-pensifar sepunya dengan peringkat p-adic yang bersepadanan dengan titik persilangan di dalam gabungan gambarajah penunjuk polihedron Newton polinomial-polinomial ini. Ini akan menghasilkan saiz pensifar-pensifar sepunya bagi f_x dan f_y. Maklumat ini kemudiannya digunakan untuk memperoleh anggaran kekardinalan di atas.

CHAPTER I

INTRODUCTION

Notation and Definition

As usual, we use the standard notation Z, Q, R and C to denote ring of integers, field of rational numbers, field of real numbers and field of complex numbers respectively. With p denoting a prime number, Z_p will denote the ring of p-adic integers, Q_p the field of p-adic numbers and Ω_p the completion of the algebraic closure of Q_p.

The lower case of Roman letters will represent elements in Z or Z_p and the Greek letter α always denotes the exponent of a prime p.

With $\underline{x}$ denoting n tuple of variable $(x_1,\ldots,x_n)$, n = 1, 2, 3,..., and F either a ring or field, $F[\underline{x}]$ will mean the ring of polynomials with coefficients in F. In our discussion F is either Z or Q_p or field extensions of Q_p

Let $\underline{f} = (f_1, \ldots, f_m)$ be m tuple of linear polynomials in $F[\underline{x}]$. If $f_i = \sum a_{ij} x_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, we call the m x n matrix $[a_{ij}]$, the matrix representing $\underline{f}$ and J_f the Jacobian matrix $\left[\frac{\partial f_i}{\partial x_j}\right]$.

Suppose f = $\sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ is a polynomial in $F[\underline{x}]$. The degree of f will be denoted by

$$\deg(f) = \max_{i_1 \ldots i_n} (i_1 + \ldots + i_n).$$

Let p be any prime number. For any nonzero integer a, $ord_p\, a$ will be the highest power of p which divides a, that is the greatest α such that $a \equiv 0 \pmod{p^\alpha}$.

If $x = a/b$ is any rational number, we define $ord_p\, x$ to be $ord_p\, a - ord_p\, b$. This resembles the property of logarithm.

Further define a map $||_p$ on Q as follows:

$$|x|_p = \begin{cases} \dfrac{1}{p^{ord_p x}} & if \quad x \neq 0 \\ 0 & if \quad x = 0 \end{cases}$$

It can be shown that $|\ |_p$ is a non-Archimedean valuation on Q (Koblitz 1977).

A sequence $\{a_i\}$ of rational numbers is called Cauchy sequence if given $\varepsilon > 0$, there exists an N such that $| a_i - a_{i'} |_p < \varepsilon$, for i, $i' >$ N. Two Cauchy sequences $\{a_i\}$ and $\{b_i\}$ are equivalent if

$$\lim_{i \to \infty} |a_i - b_i|_p = 0$$

We define the field Q_p to be the set of equivalence classes of Cauchy sequences in Q, so Q_p is the completion of Q with respect to $|\ |_p$

We denote by Q_p, the algebraically closed field of Q_p and Ω_p the completion of $\overline{Q}_p$ with respect to $|\ |_p$. It is found that the process of extending $|\ |_p$ from Q_p to $\overline{Q}_p$ and Ω_p is unique because Ω_p is algebraically closed, as well as complete.

With the above definitions, we define the Newton polygon for polynomials in p-adic field as given by Koblitz (1977) as follows :

Let $f(x) = 1 + \sum_{i=1}^{n} a_i x^i$ be a polynomial of degree n with coefficients in Ω_p and constant term 1. Consider the points (i, ord_p a_i), if $a_i = 0$, we omit that point. The Newton polygon of f(x) is defined to be the "convex hull" of this set of points which is constructed by taking a vertical line through (0, 0) and rotating it about (0, 0) counterclockwise until it hits any of the points (i, ord_p a_i) and finally hits the point (n, ord_p a_n).

Background

The role of the Newton polygon in obtaining properties of zero of polynomials in one variable is quite well known. For example, the Newton polygon can be usefully applied in proving Puiseux's theorem (Walker, 1962). A. Sathaye (1983) also consider generalise Newton-Puiseux expansion.

Koblitz (1977) discusses the Newton polygon in the p-adic case for polynomials and power series in $\Omega_p[x]$. Here estimates concerning zeros of polynomials are derived from the properties of the associated Newton polygon. In particular, if λ is the slope of a segment in the Newton polygon of a polynomial f having length N, then there are N roots of f whose p-adic order is $-\lambda$.

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

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

and denote $N(\underline{f}\,; p^\alpha)$ the cardinality of $V(\underline{f}\,; p^\alpha)$ where $\alpha > 0$ and $\underline{u}$ runs through a complete set of residues modulo p^α.

Loxton and Smith (1982) investigate the application of Newton polygon technique but finally the following method is used to arrive at their result.

With K as the algebraic number field generated by the roots ξ_i, $1 \le i \le m$ of the polynomial $f(x)$ in $Z[x]$, Loxton and Smith showed that

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

if $\alpha > \delta$, where m is the number of distinct roots of $f(x)$ and $\delta = \text{ord}_p D(f)$, where $D(f)$ denotes the intersections of the functional ideals of K generated by the number

$$\frac{f^{(e_i)}(\xi_i)}{e_i\,!}, \quad i > 1.$$

and $e = \max e_i$, with e_i as the multiplicity of the roots ξ_i.

By using a version of Hensel's Lemma, Chalk and Smith (1982) obtain a result of similar form with $\delta = \max_i \text{ord}_p f_i$ where f_i is the Taylor coefficient

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

at the distinct roots ξ_i.

Loxton and Smith (1982) show that for $\underline{f} = (f_1,\ldots,f_n)$

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

where $\delta = \text{ord}_p\, D(\underline{f})$ and $D(\underline{f})$ denotes the discriminant of $\underline{f}$, and Deg $\underline{f}$ means the product of the degrees of all the components of $\underline{f}$.

Mohd. Atan and Loxton (1986) extend the Newton polygon idea in the p-adic case to polynomials in two variables and call it Newton polyhedron method. Mohd. Atan (1986) investigates the relationships between roots of a polynomial in $\Omega_p\,[x,y]$ and its Newton polyhedron by considering the combinations of the associated indicator diagrams.

He conjectures that to every simple point of intersection in the combination of the indicator diagrams there exists common zero of both polynomials whose p-adic order corresponds to this point. He then proves that if

(λ,μ) is a point of intersection of the indicator diagrams associated with polynomials f and g in $Z_p[x,y]$, 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 $\text{ord}_p\, \xi = \lambda$, $\text{ord}_p\, \eta = \mu$.

Let A be the matrix representing $\underline{f}$ the linear polynomials with coefficients in the p-adic ring Z_p and $\alpha > 0$, Mohd. Atan (1988) shows that

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

where δ indicates the minimum of the p-adic orders of $r \times r$ non-singular submatrices of A. He also shows that

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

where f and g are linear polynomials in $Z_p[x,y]$ with $\alpha > 0$ and $\delta = \text{ord}_p\, J_{fg}$, the p-adic order of the Jacobian of f and g.

Mohd. Atan (1988) considers 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

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

in $Z_p[x,y]$ and give the estimate for $N(f_x ; f_y ; p$

p-adic orders of the coefficients of f(x,y) as follows :

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

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

Mohd. Atan and Abdullah (1992) consider 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 $\delta = \max\{\mathrm{ord}_p 3a, \mathrm{ord}_p b\}$. In both cases, the method is first to reduce both polynomials f_x, f_y to polynomials in one variable and next to consider combination of indicator diagrams associated with the p-adic Newton polyhedrons of each polynomial to determine the common zeros of the polynomials.

Mohd. Atan and Abdullah (1993) consider the same cubic polynomials and obtain a result of similar form with $\delta = \{ord_p 3a, ord_p\, b, ord_p\, c, ord_p 3d\}$. They have found 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.

Organization of The Study

In this thesis we consider the set of solutions of congruence equations modulo a prime power p associated with the polynomial

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 + mx + ny + k$$

and its cardinality is then estimated by examining the Newton polygon analogue for polynomials in $Z_p[x,y]$.

We begin in the next chapter by discussing the polynomial rings, illustrate the arithmetic operations of two polynomials and the degree for polynomial in one variable as well as polynomial with multi-indeterminates. Then we examine the relationship between the roots of polynomial and the derivatives of the same polynomial.