UNIVERSITI PUTRA MALAYSIA

AN ESTIMATION OF EXPONENTIAL SUMS ASSOCIATED WITH A CUBIC FORM POLYNOMIAL

HENG SWEE HUAY

FSAS 1999 45

AN ESTIMATION OF EXPONENTIAL SUMS ASSOCIATED WITH A CUBIC FORM POLYNOMIAL

By

HENG SWEE HUAY

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 1999

ACKNOWLEDGEMENTS

This thesis would not have been possible without the help of many who have contributed one way or another in its creation. While it is impossible to acknowledge all of them in detail, I would like to thank them all from the bottom of my heart.

However, if I may, I would like to express my most sincere appreciation to my supervisors, Dr. Hj. Ismail bin Abdullah, the Deputy Vice Chancellor.Prof. Dr. Kamel Ariffin bin Mohd. Atan and Dr. Mohamad Rushdan bin Md. Said for their valuable comments, helpful guidance and for generously providing me with an extraordinary level of support and encouragement throughout my research. The incorporation of their valuable criticisms and significant suggestions through numerous discussions was instrumental to the completion of this thesis.

To the Department of Mathematics, Universiti Putra Malaysia and to Universiti Multimedia Telekom, I would like to thank them for giving me two extremely conducive environments to carry out my research.

I would also like to dedicate this thesis to my beloved parents, whom without their love I would not be even attempting this thesis. Last but not least, I would like to thank my brothers, sisters and friends for their care, understanding and unfailing support during my course of 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
Z_p	Ring of p-adic Integer
Q_p	Field of p-adic Numbers
$\overline{Q}_p$	Algebraic Closure of Q_p
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 $(f_1, \ldots, f_m)$, $m > 1$
$\deg(\underline{f})$	Degree of $\underline{f}$
$J_{\underline{f}}$	Jacobian Matrix of $\underline{f}$
$\nabla \underline{f}$	Gradient of $\underline{f}$
N_f	Newton Polyhedron of f
$\mathrm{ord}_p a$	Highest Power of p which Divides a

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
$e_k(t)$	$e^{2\pi it/k}$
$\|\ \|_p$	Valuation respect to p
$\mid$	Divides
$\sum$	Summation
$\prod$	Product
det A	Determinant A
$V(\underline{f};p^{\alpha})$	Set $\{x \bmod p^{\alpha}: \underline{f} \equiv 0 \bmod p^{\alpha}\}$
$N(\underline{f};p^{\alpha})$	Cardinality of set $V(\underline{f};p^{\alpha})$
S(f;q)	Exponential Sums of f

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

AN ESTIMATION OF EXPONENTIAL SUMS ASSOCIATED WITH A CUBIC FORM POLYNOMIAL

By

HENG SWEE HUAY

April 1999

Chairman: **Hj. Ismail bin Abdullah, Ph.D.**

Faculty: **Faculty of Science and Environmental Studies**

With $n > 0$, $\underline{x} = (x_1, \ldots, x_n)$ and $f(\underline{x})$ is a polynomial in $Z[\underline{x}]$, the multiple exponential sum is defined to be

$$S(f;q) = \sum_{\underline{x} \bmod q} \exp(2\pi i f(\underline{x}) / q)$$

where the sum is taken over a complete set of residues modulo $q > 0$.

The method of exponential sums is one of a few general methods enabling us to solve a wide range of miscellaneous problems from the theory of numbers. The main problem of the theory of exponential sums is to obtain an upper estimate of the modulus of an exponential sum as sharp as possible.

Investigation on the sums when f is a two-variable polynomial is studied using the Newton polyhedron technique. One of the methods to obtain the estimate for

the above exponential sums is to consider the cardinality of the set of solutions to congruence equations modulo a prime power. A closer look on the actual cardinality on the following polynomial in a cubic form

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

has been carried out using the Direct Method with the aid of Mathematica. We reveal that the exact cardinality is much smaller in comparison with the estimation. The necessity to find a more precise estimate arises due to this big gap.

By a theorem of Bezout, the number of common zeros of a pair of polynomials does not exceed the product of the degrees of both polynomials. In this research, we attempt to find a better estimate for cardinality by looking at the maximum number of common zeros associated with the partial derivatives $f_x(x,y)$ and $f_y(x,y)$. Eventually a sharper estimate of cardinality for the various conditions on the coefficients of $f(x,y)$ can be determined and the estimate of $S(f; p^{\alpha})$ obtained.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains.

SATU PENGANGGARAN HASILTAMBAH EKSPONEN BERSEKUTU DENGAN SATU BENTUK POLINOMIAL KUBIK

Oleh

HENG SWEE HUAY

April 1999

Pengerusi: **Hj. Ismail bin Abdullah, Ph.D.**

Fakulti: **Fakulti Sains dan Pengajian Alam Sekitar**

Dengan $n > 0$, $\underline{x} = (x_1, \ldots, x_n)$ dan $f(\underline{x})$ suatu polinomial dalam $Z[\underline{x}]$, hasiltambah eksponen berganda ditakrifkan sebagai

$$S(f;q) = \sum_{\underline{x} \bmod q} \exp(2\pi i f(\underline{x}) / q)$$

dengan hasiltambah diambil di atas set lengkap reja modulo $q > 0$.

Kaedah hasiltambah eksponen adalah satu daripada beberapa kaedah umum yang membolehkan kita menyelesaikan berbagai masalah dalam bidang teori nombor. Persoalan utama dalam teori hasiltambah eksponen adalah untuk memperolehi satu anggaran batas atas yang setepat mungkin.

Penyelidikan hasiltambah eksponen bila f suatu polinomial dua pembolehubah dilaksanakan dengan menggunakan teknik polihedron Newton. Salah satu cara untuk mendapatkan anggaran hasiltambah eksponen di atas ialah mempertimbangkan

anggaran kepada kekardinalan set penyelesaian bagi persamaan-persamaan kongruen modulo suatu kuasa perdana. Penelitian secara lebih mendalam ke atas kekardinalan sebenar untuk polinomial berbentuk kubik berikut

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

dilaksanakan melalui Kaedah Langsung dengan bantuan pakej Mathematica. Kita dapat menunjukkan nilai bagi kekardinalan sebenar adalah jauh lebih kecil berbanding dengan nilai anggaran. Keperluan untuk mencari satu anggaran yang lebih tepat justeru timbul memandangkan jurang yang besar ini.

Melalui sebuah teorem oleh Bezout, bilangan pensifar-pensifar sepunya bagi sepasang polinomial tidak melebihi hasildarab darjah-darjah bagi kedua-dua polinomial berkenaan. Dalam penyelidikan ini, kita berusaha mencari satu anggaran kekardinalan yang lebih baik dengan meneliti bilangan maksimum pensifar-pensifar sepunya yang bersekutu dengan terbitan separa $f_x(x,y)$ dan $f_y(x,y)$. Sehubungan dengan itu satu anggaran kekardinalan yang lebih tepat dapat ditentukan melalui pelbagai syarat yang dikenakan ke atas pekai-pekali $f(x,y)$ dan seterusnya anggaran $S(f; p^{\alpha})$ diperolehi.

CHAPTER I

INTRODUCTION

Notations and Definitions

As usual, Z will denote the ring of integers, Q the field of rational numbers, R the field of real numbers and C the field of complex numbers. 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.

Generally, the lower case of Roman letters will represent elements in Z or Z_p and the Greek letter α denote the exponent of a prime p. The notation (a,b) will normally denote the greatest common divisor of a and b except occasionally will indicate an ordered pair.

With $\underline{x}$ denoting n-tuple of variable $(x_1, \ldots, x_n)$, n = 1, 2, 3, ..., and F either a ring or a 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

$1 \leq i \leq m$, $1 \leq j \leq n$, we denote the m x n coefficient matrix by $[\frac{\partial f_i}{\partial x_j}$

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

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

Finally the exponential symbol is defined as $\exp(y) = e^y$ and for a positive integer q, $e_q(t) = \exp(2\pi i t/q)$ for any t in Z.

We define the Newton polygon for polynomials in p-adic field as given by Koblitz (1977) as follows:

Let $f(x) = 1 + \sum_{i=1}^{n} a_i x^n$ be a polynomial of degree n with coefficients in Ω_p and constant term 1. Consider the points $(i, \mathrm{ord}_p a_i)$, if $a_i = 0$, we omit that point or we think of it as lying infinitely far above the horizontal axis. The Newton polygon of f(x) is defined to be the convex hull of this set of points that is the highest convex polygonal line joining (0,0) with $(n, \mathrm{ord}_p a_n)$ which passes on or below all of the points $(i, \mathrm{ord}_p a_i)$. This convex hull is constructed by rotating a vertical line through (0,0) counterclockwise until it hits any of the points $(i, \mathrm{ord}_p a_i)$ and finally hits the point $(n, \mathrm{ord}_p a_n)$.

Background

For each positive integer q and for each polynomial f in $Z[\underline{x}]$ of degree greater than 1 we define the exponential sums by

$$S(f;q) = \sum e_q(f(\underline{x}))$$

where the sum is taken over a complete set of residues $\underline{x}$ modulo q. The study of this sum is motivated by applications in analytic number theory.

The sum S(f;q) where f is a non-linear polynomial in Z[x] were investigated by authors such as Hardy and Littlewood, Deligne, Loxton and Vaughan and others. The sum S(f;q) in one-variable case were investigated by Hardy and Littlewood in connection with Waring's problem.

In 1940, Hua proved that for arbitrary $\varepsilon > 0$

$$|S(f;q)| \leq cq^{1+\varepsilon-1/n}$$

for some positive constant c which is dependent only on ε and n.

Hua's result is improved by Jing-Run Chen who shows that if the content of f - f(0) is relatively prime to q then

$$|S(f;q)| \leq e^{7(n+1)}q^{1-1/(n+1)}.$$

Hua's estimate is used by Stechkin to show that

$$|S(f;q)| \leq c^n q^{1-1/n} (c(f),q)^{1/m}$$

for some absolute positive constant c, where c(f) is the content of f - f(0).

For a prime p, Deligne (1974) showed that

$$|S(f;p)| \leq (m-1)^n p^{n/2}$$

in his proof of the Weil conjectures, where m denotes the total degree of the associated polynomial f, under the condition that the homogeneous part of f of highest degree is non-singular modulo p. His work paves the way to precise estimates of S(f;q) for general polynomials f in several variables. Loxton and Vaughan (1985) for example found very precise estimate for the sum in terms of invariants associates with a one-variable polynomial f. However, the general results for polynomials of several variables are less complete.

The Newton polygon plays an important role in ascertaining the properties of roots of polynomials in one-variable. For example, the Newton polygon method can be usefully applied in proving Puiseux's theorem on the power series development of algebraic functions. In the p-adic case, the Newton polygon yields complete information on the sizes and number of zeros of polynomials in one-variable with coefficients in Ω_p the algebraic closure of the field of p-adic numbers Q_p.

Koblitz (1977) introduces the Newton polygon in the p-adic case for polynomials and power series in $\Omega_p[x]$. He shows that the slopes of the edges of the Newton polygon give the p-adic ordinals of the reciprocal roots of f(x), with their

multiplicities. Thus the Newton polygon allows us to see at a glance at what radii the reciprocal roots are located. More precisely, if the Newton polygon has an edge joining $(i,\mathrm{ord}_p a_i)$ to $(j,\mathrm{ord}_p a_j)$ with $j > i$, then f has exactly $(j - i)$ roots with p-adic orders $\dfrac{\mathrm{ord}_p a_j - \mathrm{ord}_p a_i}{j-i}$.

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.

Let K be 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 show that

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

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

$$\frac{f^{(e_i)}(\xi_1)}{e_1!},$$

$i > 1$ and $e = \max e_i$ with e_i 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 $\delta = \max_i \mathrm{ord}_p f_i$ 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 $\underline{f} = (f_1, \ldots, f_n)$

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

where $\delta = \mathrm{ord}_p D(\underline{f})$ 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-variable and call it Newton polyhedral method. We list out a few results that had been developed recently which are centred in the use of the Newton polyhedral method to arrive at the estimates.

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

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

where δ indicates the minimum of the p-adic orders of r x r non-singular submatrices of A. He also shows in a specific case that when n = 2,

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

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 $f = (f_x, f_y)$ 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 $Z_p[x,y]$, with $p > 2$ and gives the estimate for $N(f;p^{\alpha})$ explicitly in terms of the p-adic orders of the coefficients of f(x,y) as follows:

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

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

Mohd. Atan and Abdullah (1992) consider the more general cubic polynomial

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

and obtain the result of similar form as above with $\delta = \max\{\text{ord}_p 3a, \text{ord}_p b\}$. Mohd. Atan and Abdullah (1993) complete the investigation on the same cubic polynomial and again obtain a result of similar form with the new determining factor $\delta = \max\{\text{ord}_p 3a, \text{ord}_p b, \text{ord}_p c, \text{ord}_p 3d\}$. This shows that the determinant factor is in fact dependent on the dominant terms of f(x,y).

Finally, Chan (1997) obtains the estimate for $N(f; p^{\alpha})$ of a polynomial with degree higher than the one considered above of the form

$$f(x,y) = ax^4 + bx^3y + cxy^3 + mx + ny + k$$

in $Z_p[x,y]$ with $p > 3$ and he obtains the estimate as follows :

$$N(f_x, f_y; p^{\alpha}) \leq \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 9p^{2/3(2\alpha+\delta)} & \text{if } \alpha > \delta \end{cases}$$

where $\alpha > 0$ and $\delta = \max\{\text{ord}_p a, \frac{3}{2}\text{ord}_p b, \frac{3}{2}\text{ord}_p c\}$. He continues the research and obtains a similar result for a complete quartic polynomial of the form

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

in $Z_p[x,y]$ with $p > 3$ and $\delta = \max\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p d, \text{ord}_p e\}$. This gives a more symmetric result than the previous one.

Organisation of the Study

This thesis is concerned with finding a more precise estimate for the cardinality and exponential sums of the polynomials in a cubic form

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

Initially, a comparison is done between the estimation and the actual cardinality. The necessity to find a sharper upper estimate arises due to the big gap between the values of the two methods. By considering the various conditions on the coefficients and the number of distinct common zeros associated with both the partial derivatives $f_x(x,y)$