UNIVERSITI PUTRA MALAYSIA

EXPONENTIAL SUMS FOR SOME HIGHER DEGREE POLYNOMIALS

LOW CHEE WAI

IPM 2019 18

EXPONENTIAL SUMS FOR SOME HIGHER DEGREE POLYNOMIALS

By

LOW CHEE WAI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Master of Science

December 2018

DEDICATIONS

To all of my love:
Father
Mother
Sister
Lecturers
Friends
...

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the Master of Science

EXPONENTIAL SUMS FOR SOME HIGHER DEGREE POLYNOMIALS

By

LOW CHEE WAI

December 2018

Chairman: Siti Hasana binti Sapar, PhD
Institute: Institute for Mathematical Research

Let $f(x, y)$ be a polynomial of two variables in $\mathbb{Z}_p[x, y]$ and p be a prime. Suppose $\alpha > 1$, the exponential sums of polynomial $f(x, y)$ is defined by

$$S(f; p^{\alpha}) = \sum_{x,y \bmod p} e^{\frac{2\pi i f(x,y)}{p^{\alpha}}},$$

where the sum is taken over a complete set of residue modulo p. In order to get the value of $S(f; p^{\alpha})$, the cardinality $N(g, h; p^{\alpha})$ and the p-adic sizes must be obtained first. This thesis discuss the finding of p-adic sizes of common zeros of the partial derivative polynomials f_x, f_y which derive from $f(x, y)$ by using Newton polyhedron technique. Then, the estimation of the cardinality and exponential sums of polynomial $f(x, y)$ will be determined by considering four different polynomials, that are degree five, six, seven and eight.

The Newton polyhedron technique is a method to estimate the p-adic sizes of common zeros of partial derivative polynomials. This method is to get the Newton polyhedron for the partial derivative polynomials. Then, the indicator diagram for each of the partial derivative polynomials will be constructed. Each of the intersection point in the combination of indicator diagram gives the p-adic sizes of the common zeros associated with the considered partial derivative polynomials.

This research found that the exponential sums for the polynomials of degree five, six, seven and eight are

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 16p^{\alpha+1+44\delta+8q}\},$$

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 25p^{\alpha+1+56\delta+10q}\},$$

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 36p^{\alpha+1+68\delta+12q}\}$$

and

$$|S(f;p^\alpha)| \leq \min\{p^{2\alpha}, 49p^{\alpha+1+80\delta+14q}\}$$

respectively where $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Sarjana Sains

HASIL TAMBAH EKSPONEN BAGI SUATU POLINOMIAL BERDARJAH TINGGI

Oleh

LOW CHEE WAI

Disember 2018

Pengerusi: Siti Hasana binti Sapar, PhD
Institut: Institut Penyelidikan Matematik

Biarkan $f(x, y)$ suatu polinomial dua pembolehubah dalam $\mathbb{Z}_p[x, y]$ dan p suatu nombor perdana. Katakan $\alpha > 1$, hasil tambah eksponen bagi polinomial $f(x, y)$ ditakrifkan sebagai

$$S(f; p^{\alpha}) = \sum_{x,y \bmod p} e^{\frac{2\pi i f(x,y)}{p^{\alpha}}}$$

yang mana hasil tambah diambil dalam satu set reja lengkap modulo p. Bagi mendapatkan nilai $S(f; p^{\alpha})$, kekardinalan $N(g, h; p^{\alpha})$ dan saiz p-adic mesti diperoleh terlebih dahulu. Tesis ini akan membincangkan untuk mendapatkan saiz p-adic bagi pensifar sepunya polinomial terbitan separa f_x, f_y yang diperolehi daripada $f(x, y)$ dengan menggunakan teknik polihedron Newton. Kemudian, penganggaran bagi kekardinalan dan hasil tambah eksponen bagi polinomial $f(x, y)$ akan ditentukan dengan mempertimbangkan empat polinomial yang berbeza, iaitu berdarjah lima, enam, tujuh dan lapan.

Teknik polihedron Newton ialah suatu kaedah untuk menganggarkan saiz p-adic persifar sepunya polinomial terbitan separa. Kaedah ini ialah untuk mendapatkan polihedron Newton bagi polinomial terbitan separa. Kemudian, gambar rajah penunjuk bagi setiap terbitan separa polinomial akan dibina. Setiap titik persilangan pada gabungan gambar rajah penunjuk memberi saiz p-adic persifar sepunya yang disekutukan dengan polinomial terbitan separa yang dipertimbangkan.

Kajian ini didapati bahawa hasil tambah eksponen bagi polinomial berdarjah lima, enam, tujuh dan lapan ialah

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 16p^{\alpha+1+44\delta+8q}\},$$

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 25p^{\alpha+1+56\delta+10q}\},$$

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 36p^{\alpha+1+68\delta+12q}\}$$

dan

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 49p^{\alpha+1+80\delta+14q}\}$$

masing-masing di mana $q = \max\{\epsilon_1, \epsilon_3 + \frac{1}{2}\omega_0\}$.

ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude to my academic supervisor, Assoc. Prof. Dr. Siti Hasana binti Sapar who gave me the opportunity to do this research. She has always guided me and kept me on the right track in completing this research as well as to check and correct my mistakes. I learnt many things and gained many knowledge throughout the research. I was not familiar with the field that I am going to do at the beginning, then I was able to understand parts by partsafter her advice and guidance.

Next, I would like to give a special thank to my co-supervisor, Dr. Mohamat Aidil bin Mohamat Johari for willing to spend time to read and check my works. Besides, I thank to my institute whcih is INSPEM for providing a good working place and facilities that helped me a lot in finding the information. Also, INSPEM provided a series of seminars and workshops for us in order to help us in our research. Thanks to the staffs and lecturers in helping me when I need help.

In addition, I thank Graduate Research Fund (GRF) for the financial support as I go through the research. I thank to my family who gave me tremendous moral supportin enduring the hardship and stress.

Last but not least, I want to thank my friends for supporting me to continue my study in master degree and gave me support throughout the research. Their support really gave me the motivation to continue my research.

I appreciate the help from all of them and I am very grateful to have these people in my life. Thank you so much.

I certify that a Thesis Examination Committee has met on 26 December 2018 to conduct the final examination of Low Chee Wai on his thesis entitled "Exponential Sums for Some Higher Degree Polynomials" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Norfifah bt Bachok @ Lati, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Sharifah Kartini bte Said Husain, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Eddie Shahril Ismail, PhD
Associate Professor
School of Mathematical Sciences
National University of Malaysia
Malaysia
(External Examiner)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 October 2019

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Siti Hasana binti Sapar, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

Mohamat Aidil bin Mohamat Johari, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ______________________ Date: ______________________

Name and Matric No.: ______________________________________

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ____________________
Name of
Chairman of
Supervisory
Committee: ____________________

Signature: ____________________
Name of
Member of
Supervisory
Committee: ____________________

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

LIST OF ABBREVIATIONS

p	Prime number
α	Exponent of prime number
$\mathbb{Z}$	Positive integer
$\mathbb{Q}$	Rational number
$\mathbb{C}$	Complex coefficient
$\mathbb{R}$	Real number
$\mathbb{Z}_p$	Ring of p-adic integer
$\mathbb{Q}_p$	Field of rational p-adic number
Ω_p	Completion of the algebraic closure of p-adic field
Ω_p^n	Neighbourhood of points in Ω_p
$S(f;q)$	Exponential Sums
$N(f_x, f_y; p^\alpha)$	Cardinality of set $V(f_x, f_y; p^\alpha)$
$f(x)$	Polynomial with one-variable
$f(x, y)$	Polynomial with two-variable
$D(\nabla F)$	Dimension of the gradient of continuous function F
min	Minimum
max	Maximum
$ord_p\ a$	Highest power of p which divides a
inf	Infimum
mod	Modulo
exp	Exponent

CHAPTER 1

INTRODUCTION

1.1 Background

In this chapter, we are going to give a brief background about what is exponential sums, cardinality and p-adic sizes. The following definition explains the exponential sums.

Definition 1.1.1 *The exponential sums of a polynomial f is given by*

$$S(A) = \sum_{x} e^{2\pi i f(x)} \tag{1.1}$$

where x runs all over integer from certain interval A and $f(x)$ is a polynomial taking on real values under integer x.

In number theory, estimation of exponential sums can be used in solving the Waring's problems (Korobov (1992)) and communication theory (Paterson (1999)) in cryptography.

Next, the following definition explains the cardinality.

Definition 1.1.2 *Let $N(f_x, f_y; p^\alpha)$ denotes as the cardinality of the set*

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

of polynomial in $\mathbb{Z}_p[x, y]$. The cardinality represents the number of common solutions for the following congruence equations in the complete set of residue modulo p^α

$$f_x(x, y) \equiv 0 \ (mod\ p^\alpha)$$

and

$$f_y(x, y) \equiv 0 \ (mod\ p^\alpha)$$

where f_x and f_y are the partial derivative of the polynomial $f(x, y)$ with respect to x and y respectively.

The p-adic size of an integer a is denoted by $ord_p\ a$ and it is defined by the following definition.

Definition 1.1.3 *Let p be any prime number and a be any nonzero integer. Then* $ord_p\ a$ *is defined as the highest power of p which divides a.*

In other words, if $a = b \cdot p^n$ where n is an integer and $p \nmid b$, then $ord_p\ a = n$. The following definitions state the p-adic integer.

Definition 1.1.4 *Let* x *be an element in* $\mathbb{Q}_p$ *where* $p \geq 2$ *is a prime, then* x *is in* $\mathbb{Z}_p$ *if and only if*

$$x = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$$

where $|a|_p = p^{-\beta}$ *and* β *is the p-adic sizes of a.*

Definition 1.1.5 *Let* $p \geq 2$ *be a prime. For any integer* $n > 0$*, the p-adic interger of n is a series in base p given as followed:*

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$$

with $a_0, a_1, a_2, \ldots, a_k$ *are integers such that* $0 \leq a_i < p$.

Example 1.1.1 *Let 516 be an element of 3-adic, then 516 can be expressed as follow:*

$$516 = 0(3)^0 + 1(3)^1 + 0(3)^2 + 1(3)^3 + 0(3)^4 + 2(3)^5.$$

However, $\mathbb{Z}_p$ is defined as $\mathbb{Z}_p = \{[0]_p, [1]_p, [2]_p, \ldots, [p-1]_p\}$. If $p = 3$, then $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ with

$$[0]_3 = \{x | x = 0 + 3k, k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$

$$[1]_3 = \{x | x = 1 + 3k, k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$

$$[2]_3 = \{x | x = 2 + 3k, k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Therefore, $516 \in \mathbb{Z}_3$ since $516 = 0 + 3(172) \in [0]_3$.

Now, the extension of $\mathbb{Z}_p$ to $\mathbb{Q}_p$ by considering the rational numbers. An example of elements in $\mathbb{Q}_p$ is $\frac{1}{3} = 1(3)^{-1} + 0(3)^0 + 0(3)^1 + 0(3)^2 + \ldots$ with $p = 3$.

Ω_p denotes the completion of the algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. In other words, it is the field of the complex p-adic numbers. For instance, $19 + 83i = (1 + i)(51 + 32i)$ with $p = 1 + i$.

$\bar{\mathbb{Q}}_p[x,y]$ is the algebraic closure of $\mathbb{Q}_p$. Thus, it also a field. The difference between $\bar{\mathbb{Q}}_p$ and $\mathbb{Q}_p$ is that every polynomial in $\bar{\mathbb{Q}}_p$ can be splited completely over $\bar{\mathbb{Q}}_p$. That is, $\bar{\mathbb{Q}}_p$ contain all the elements that are algebraic over $\mathbb{Q}_p$.

1.2 Literature Review

Koblitz (1977) introduced Newton polygon method for polynomials and power series in $\Omega_p[x]$ where Ω_p denotes the completion of the algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. He developed some basic concepts about p-adic analysis together with the applications of it. It was then became a very interesting topic in number theory.

Deligne (1974) discovered that for any prime p,

$$|S(f;p)| \leq (m-1)^n p^{\frac{n}{2}} \tag{1.2}$$

where $n > 1$ denotes as the number of variables of the polynomial f and m is the total degree of f. This makes the estimation of exponential sums become more accurate and precise.

Loxton and Smith (1982) improved the results of Deligne. They found that the estimation of exponential sums is given by

$$|S_F(p^\alpha)| \leq m^n p^{\frac{n\alpha}{2}} (D(\nabla F)^5, p^\alpha)^{\frac{n}{2}} \tag{1.3}$$

where p is a prime, $\alpha > 1$ and dimension of the gradient of continuous function F, $D(\nabla F) \neq 0$. This estimation is used for $m+1$ degree non-linear polynomial f in $\mathbb{Z}[x]$.

Next, Mohd Atan (1985) used the Newton polyhedron method to estimate the exponential sums associated with the polynomial $f(x,y) = ax^3 + bx^2y + cx + dy + e$ in the ring of p-adic integers.

Mohd Atan (1986a) extended the idea of Newton polygon to Newton polyhedron method for the polynomials with two variables. He figured out that if a point (ξ, η) is a zero of a polynomial f in Ω_p where p is a prime, then the plane $(ord_p\ \xi, ord_p\ \eta, 1)$ is a normal to an edge in the Newton polyhedron of a polynomial f denoted by N_f that falls between the upward-pointing normals to the faces of N_f adjacent to this edge. The same research also found that the $ord_p\ \xi$ and $ord_p\ \eta$ can be estimated by using these edges and faces.

In the same year, Mohd Atan (1986b) studied the combination of the indicator diagram of two polynomials and found that the p-adic sizes of both polynomials can be estimated from the intersection points of segment in the indicator diagram. He constructed the following conjecture:

Conjecture 1.1.1 Let f and g be polynomials in $\bar{\mathbb{Q}}_p[x, y]$ and let (λ, μ) be a point of intersection of their indicator diagrams and suppose that the edges through (λ, μ) do not coincide. Then there are ξ and η in $\bar{Q}_p[x, y]$ satisfying $f(\xi, \eta) = g(\xi, \eta) = 0$ and $ord_p\ \xi = \lambda,\ ord_p\ \eta = \mu$.

Mohd Atan (1988) obtained the estimation of cardinality of a polynomial by using Newton polyhedron method. He proved that the cardinality of the polynomials $f(x, y) = 3ax^2 + by^2 + c$ and $g(x, y) = 2bxy + d$ is given by

$$card\ V_i(f; g; p^\alpha) \leq p^{\alpha+\delta}.$$

Mohd Atan (1990) continued his research on finding the exponential sums of a polynomial. He found that the cardinality of the set of solutions to the congruence equation modulo $p^{\frac{\alpha}{2}}$ for positive even α can be used to estimate the exponential sums of a polynomial.

Mohd Atan and Abdullah (1993) found the solution of polynomial

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

in $\mathbb{Z}_p[x, y]$ by using the Newton polyhedron method. The two polynomials that formed on the indicator diagram are the polynomials that differentiated from f with respect to x and y. The intersection point on the indicator diagram is $\left(\frac{1}{2}ord_p(3a + b\alpha), \infty\right)$ for $\alpha > 0$. They found that the cardinality is given by

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

Mohd Atan (1995) studied the works of Deligne (1974) as well as Loxton and Smith (1982) by considering the polynomial of the form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3ex + my + n$. He found that

$$|S(f; p^\alpha)| \leq p^{2(\alpha-\delta)} \min\{p^{2\delta}, 4p^{\delta+\alpha}\}$$

if α is even and $\alpha = 2\delta$,

$$|S(f; p^\alpha)| \leq p^{\alpha+\frac{1}{2}} \min\{p^{2\delta}, 4p^{\delta+\alpha}\}$$

if α is odd and $\alpha = 2\delta + 1$.

Heng and Mohd Atan (1999) investigated the cardinality of the set of solutions for polynomial $f(x,y) = ax^3 + bxy^2 + cx + dy + e$. The cardinality is given by

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

where $p > 3$ is a prime, $\alpha > 1$ and $\delta = \min\{ord_p\ 3a, \frac{3}{2}\ ord_p\ b\}$.

Sapar and Mohd Atan (2002) studied the estimation of cardinality of the set of solutions for some polynomials. The polynomials chosen are the second and third degree polynomials. They used the indicator diagram and Newton polyhedron method in order to obtain the cardinality of the polynomials.

Sapar and Mohd Atan (2006) continued their research by considering the following polynomial:

$$f(x,y) = ax^5 + bx^4y + cx^3y^2 + dx^2y^3 + exy^4 + my^5 + nx + ty + k$$

with $ord_p\ b^2 > ord_p\ ac$ and $ord_p(10cm - 2de)^2 > ord_p(10dm - 4e^2)(2ce - d^2)$. They found that the p-adic sizes of common zeros of partial derivatives of the polynomial above is given by

$$ord_p\ \xi \geq \frac{1}{4}(\alpha - \delta),\ ord_p\ \eta \geq \frac{1}{4}(\alpha - \delta).$$

Nevertheless, Sapar and Mohd Atan (2007) considered a sixth degree polynomial $f(x,y) = ax^6 + bx^5y + cx^4y^2 + dx^3y^3 + ex^2y^4 + mxy^5 + ny^6 + sx + ty + k$ with the condition $ord_p(120ck - 8e^2)^2 > ord_p\ 4(90dk - 20em)(20cm - 6de)$. They used the Newton polyhedron method to estimate the p-adic sizes of common zeros of partial derivative of the polynomial. The results found are

$$ord_p\ \xi \geq \frac{1}{5}(\alpha - \delta),\ ord_p\ \eta \geq \frac{1}{5}(\alpha - \delta).$$

Then, Sapar and Mohd Atan (2009) consider another polynomial of quintic form given by

$$f(x,y) = ax^5 + bx^4y + cx^3y^2 + sx + ty + k$$

with $ord_p\ b^2 > ord_p\ ac$ and certain conditions. The results are quite similar to the works in Sapar and Mohd Atan (2006).

Yap (2010) studied the estimation of exponential sums for a polynomial f using p-adic sizes that obtained from the indicator diagram. He found that the exponential sums is given by

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 4p^{\frac{3}{2}\alpha+\delta}\}$$

and

$$|S(f;p^{\alpha})| \leq \min\{p^{2\alpha}, 4p^{\frac{3}{2}\alpha+\delta+\epsilon}\}$$

for some $\epsilon > 0$.

One year later, Yap et al. (2011) studied the p-adic sizes of a polynomial associated with cubic form. They found that the p-adic sizes are given by

$$ord_p(\xi - x_0) \geq \frac{1}{2}(\alpha - \delta),\ ord_p(\eta - y_0) \geq \frac{1}{2}(\alpha - \delta).$$

This estimation is valid for the neighbourhood of (x_0, y_0) of common zeros (ξ, η) of the partial derivative polynomials associated with cubic form

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

in $\mathbb{Z}_p[x,y]$ and (x_0, y_0) in Ω_p^2.

Sapar et al. (2013) studied the p-adic sizes of a polynomial with degree nine in the form of $f(x,y) = ax^9 + bx^8y + cx^7y^2 + sx + ty + k$. They found that there exist (ξ, η) in such a way that $f_x(\xi, \eta) = 0$ and $f_y(\xi, \eta) = 0$ by using the Newton polyhedron method. The results are

$$ord_p(\xi) \geq \frac{1}{8}(\alpha - \delta)$$

and

$$ord_p(\eta) \geq \frac{1}{8}(\alpha - \delta)$$

or in an exceptional case

$$ord_p(\eta) \geq \frac{1}{2}(\alpha - \delta - \epsilon)$$

for certain $\epsilon > 0$.

Aminudin et al. (2014) considered a polynomial of degree eight. In this research, they found that the results are not unique due to they considered all the possible cases that happened during their researh. The polynomial that they chosen is

$$f(x,y) = ax^8 + bx^7y + cx^6y^2 + sx + ty + k.$$

Zulkapli et al. (2015) investigated the p-adic sizes of factorials. The results obtained are in explicit forms and the method of obtaining them offers an alternative way in finding $ord_p\ n!$. Other than that, they found the p-adic sizes of ${}^nC_r$ where $n = p^\alpha$ and $r = p^\theta$ for $\alpha > \theta > 0$.

Lasaraiya et al. (2016a) investigated the cardiality of twelfth degree polynimial in the form $f(x, y) = ax^{12} + bx^{11}y + cx^{10}y^2 + sx + ty + k$. The result is as follows:

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 121p^{2(11\delta + \frac{3}{2}\epsilon_0 + 9\epsilon_1 + 11q)} & \text{if } \alpha > \delta \end{cases}$$

where $p > 11$ is a prime, $\alpha > 1$, $\epsilon_0, \epsilon_1, q \geq 0$ and $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c\}$.

Last but not least, Lasaraiya et al. (2016b) studied the cardinality of the polynomial of degree eleven in the form $f(x, y) = ax^{11} + bx^{10}y + cx^9y^2 + sx + ty + k$. They found out that the cardinality is given by

$$N(f_x, f_y; p^\alpha) = \begin{cases} p^{2\alpha} & \text{if } \alpha \leq \delta \\ 100p^{2(9\delta + \frac{3}{2}\epsilon_0 + 8\epsilon_1 + 10q)} & \text{if } \alpha > \delta \end{cases}$$

where $p > 11$ is a prime, $\alpha > 1$, $\epsilon_0, \epsilon_1, q \geq 0$ and $\delta = \max\{ord_p\ a, ord_p\ b, ord_p\ c\}$.

1.3 Problem Statement

For the past 40 years, many researchers that we mentioned in previous section (1.2 Literature Review) involved in finding the p-adic sizes, cardinality and exponential sums for different polynomials. Since every different polynomials give different p-adic sizes, the cardinality and the exponential sums are also different. Thus, researchers are thinking of finding the p-adic sizes in more general so that we can obtain the exponential sums more precise and systematic. In such a way, we are going to investigate the exponential sums of polynomial with dominant terms for degree of n. So we started by considering the polynomials of degree five, six, seven and eight.

1.4 Research Objectives

The objectives of this research are as follow:

- To estimate the p-adic sizes of common zeros associated with the polynomials of degree five, six, seven and eight.
- To determine the estimation of the cardinality of the sets of solutions to congruence equations of these polynomials.
- To determine the estimation of the exponential sums of the polynomials under consideration.

1.5 Research Methodology

We used the Newton polyhedron method to find the estimation of p-adic sizes of the fifth, sixth, seventh and eighth degree polynomials respectively. Then, the combination of the indicator diagram associated with the partial derivative polynomials is constructed and analyzed. Finally, we find the cardinality and the exponential sums of the polynomials after we get the results of p-adic sizes of every polynomial that we considered.

1.6 Organization of Thesis

This thesis covers six chapters as follows:

Chapter 1 provides a brief introduction of this research. The previous researches done by other researchers of the related topic as it gone throught. This chapter also includes the problem statement, objectives and methodology of this research.

Chapter 2 explains the method that we are going to use for this research. In this chapter, we explain more detail about the Newton polyhedron method as well as the indicator diagram. We provide one polynomial as an example throught out this chapter to help readers understand how the method being used.

Chapter 3 is the main part of our research. We are going to obtain the estimation of the p-adic sizes of the fifth, sixth, seventh adn eighth degree polynomials that we considered. The results of the estimation will be different due to different conditions.

Chapter 4 and chapter 5 are going to present the estimation of the cardinality and the exponential sums of the polynomials that we considered respectively. In the finding of exponential sums, we will consider two cases which are when α is even and when α is odd.

In the last chapter which is Chapter 6, we provide a summary of what we have done and the results of the research. Also, some future works and recommendation will be discussed in the last part of this chapter.

REFERENCES

Aminudin, S. S., Sapar, S. H. and Mohd Atan, K. A. 2014. On the Cardinality of the Set of Solutions to Congruence Equation Associated with Cubic Form. *JP Journal of Algebra, Number Theory and Applications* 33 (1): 1.

Deligne, P. 1974. La conjecture de Weil. *Inst. Hautes Etudes Sci. Publ. Math* 43 (1): 273–307.

Heng, S. H. and Mohd Atan, K. A. 1999. An Estimation of Exponential Sums Associated with a Cubic Form. *Physical Sci* 10: 1–21.

Koblitz, N. 1977, In p-adic Numbers, p-adic Analysis, and Zeta-Functions, In *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 1–20, Springer, 1–20.

Korobov, N. M. 1992, In Exponential Sums and Their Applications, In *Exponential Sums and Their Applications*, 1–67, Springer, 1–67.

Lasaraiya, S., Sapar, S. H. and Johari, M. A. M. 2016a. On the Cardinality of Twelfth Degree Polynomial. In *AIP Conference Proceedings*, 020008. AIP Publishing.

Lasaraiya, S., Sapar, S. H. and Johari, M. A. M. 2016b. On the Cardinality of the Set of Solutions to Congruence Equation Associated with Polynomial of Degree Eleven. In *AIP Conference Proceedings*, 050015. AIP Publishing.

Loxton, J. H. and Smith, R. A. 1982. Estimates for Multiple Exponential Sums. *Journal of the Australian Mathematical Society* 33 (1): 125–134.

Mohd Atan, K. A. 1985. Newton Polyhedra and Estimates for Exponential Sums. *Bull. Austral. Math. Soc* 12: 10G10.

Mohd Atan, K. A. 1986a. Newton Polyhedra and p-adic Estimates of Zeros of Polynomials in Np[x,y]. *Pertanika* 9 (1): 51–56.

Mohd Atan, K. A. 1986b. 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 Set of Solutions to Congruence Equations. *Pertanika* 11 (1): 125–131.

Mohd Atan, K. A. 1990. Satu Kaedah Menganggar Hasil Tambah Eksponen Berganda. *Matematika Jabatan Matematik UTM* 6: 37–48.

Mohd Atan, K. A. 1995. An Explicit Estimate of Exponential Sums Associated with a Cubic Polynomial. *Acta Mathematica Hungarica* 69 (1-2): 83–93.

Mohd Atan, K. A. and Abdullah, I. 1993. On the Estimate to Solutions of Congruence Equations Associated with a Cubic Form. *Pertanika Journal of Science and Technology* 1 (2): 249–260.

Paterson, K. G. 1999. Applications of Exponential Sums in Communications Theory. In *IMA International Conference on Cryptography and Coding*, 1–24. Springer.

Sapar, S. H. and Mohd Atan, K. A. 2002. Estimate for the Cardinality of the Set of Solution to Congruence Equations. *Journal of Technology* 36: 13–40.

Sapar, S. H. and Mohd Atan, K. A. 2006. Estimation of p-adic Sizes of Common Zeros of Partial Derivative Polynomials Associated with a Quintic Form. *Jurnal Teknologi UTM* 45 (C): 85–96.

Sapar, S. H. and Mohd Atan, K. A. 2007. Penganggaran Saiz p-adic Pensifar Sepunya Terbitan Separa Polinomial Berdarjah Enam. *Sains Malaysiana* 36 (1): 77–82.

Sapar, S. H. and Mohd Atan, K. A. 2009. A Method of Estimating the p-adic Sizes of Common Zeros of Partial Derivative Polynomials Associated with a Quintic Form. *International Journal of Number Theory* 5 (03): 541–554.

Sapar, S. H., Mohd Atan, K. A. and Aminuddin, S. S. 2013. An Estimating the p-adic Sizes of Common Zeros of Partial Derivative Polynomials. *New Trends in Mathematical Sciences* 1 (1): 38–48.

Yap, H. K. 2010. *Estimation of Exponential Sums Using p-adic Methods and Newton Polyhedron Technique*. PhD thesis, Universiti Putra Malaysia.

Yap, H. K., Mohd Atan, K. A. and Sapar, S. H. 2011. Estimation of p-adic Sizes of Common Zeros of Partial Derivatives Associated with a Cubic Form. *Sains Malaysiana* 40 (8): 921–926.

Zulkapli, R., Mohd Atan, K. A. and Sapar, S. H. 2015. A Method for Determining p-adic Orders of Factorials. *Malaysian Journal of Mathematical Sciences* 9 (2): 277–300.

BIODATA OF STUDENT

The student, Low Chee Wai, was born on the 16th of May 1991 in Kuala Lumpur. The student started his education in Sekolah Jenis Kebangsaan (Cina) Chin Woo, Kuala Lumpur in 1998. He continue his secondary education in Sekolah Menangah Kebangsaan Datok Lokman in Kampong Pandan, Kuala Lumpur. After finish his secondary education in 2009, he choose to continue Form 6 as Pre-U programme in the same school. In 2012, he received the offer from Universiti Putra Malaysia. The course offer was Bachelor of Science (Honours) majoring in Mathematics. He graduated in June 2016 and started his Master Degree in September 2016.

The student can be contacted through his supervisor, Assoc. Prof. Dr. Siti Hasana binti Sapar, by address:

Department of Mathematics,
Faculty of Science,
Universiti Putra Malaysia,
43400 Serdang,
Selangor,
Malaysia.

Email: sitihas@upm.edu.my
Contact number: +603-8946 8456

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : First Semester 2019/2020

TITLE OF THESIS / PROJECT REPORT :

EXPONENTIAL SUMS FOR SOME HIGHER DEGREE POLYNOMIALS

NAME OF STUDENT: LOW CHEE WAI

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☐	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐	**PATENT**	Embargo from_____________ until _____________ (date) (date)

Approved by:

(Signature of Student) New IC No/ Passport No.:	(Signature of Chairman of Supervisory Committee) Name:
Date :	Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]