UNIVERSITI PUTRA MALAYSIA

PENGANGGARAN KEKARDINALAN BAGI SET PENYELESAIAN SISTEM PERSAMAAN KONGRUEN MELALUI KAEDAH TRANSFORMASI

SHARIFAH KARTINI BINTI SAID HUSAIN

FSAS 2000 3

PENGANGGARAN KEKARDINALAN BAGI SET PENYELESAIAN SISTEM PERSAMAAN KONGRUEN MELALUI KAEDAH TRANSFORMASI

SHARIFAH KARTINI BINTI SAID HUSAIN

MASTER SAINS
UNIVERSITI PUTRA MALAYSIA

2000

PENGANGGARAN KEKARDINALAN BAGI SET PENYELESAIAN SISTEM PERSAMAAN KONGRUEN MELALUI KAEDAH TRANSFORMASI

Oleh

SHARIFAH KARTINI BINTI SAID HUSAIN

Tesis Yang Dikemukakan Sebagai Memenuhi Keperluan Untuk
Ijazah Master Sains
di Fakulti Sains dan Pengajian Alam Sekitar
Universiti Putra Malaysia

September 2000

DEDIKASI

Teristimewa buat

Ibuku, Tuan Nong binti Syed Abdullah

abang-abang, kakak-kakak

dan anak-anak saudara

dan dihadiahkan kepada

Syed Ahmad Thani bin Tuan Hadi

dan Sharifah Maisara

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

PENGANGGARAN KEKARDINALAN BAGI SET PENYELESAIAN SISTEM PERSAMAAN KONGRUEN MELALUI KAEDAH TRANSFORMASI

Oleh

SHARIFAH KARTINI BINTI SAID HUSAIN

SEPTEMBER 2000

Pengerusi: Dr. Hj. Ismail bin Abdullah

Fakulti: Sains dan Pengajian Alam Sekitar

Penganggaran kekardinalan bagi set penyelesaian bagi persamaan kongruen modulo suatu kuasa perdana p yang disekutukan dengan suatu polinomial kuartik berbentuk

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

dalam $Z_p[x,y]$ ditentukan dengan menggunakan kaedah transformasi.

Kaedah ini digunakan apabila berlaku beberapa kes atau keadaan polinomial, iaitu:

1. Polinomial atau sepasang polinomial tak linear.
2. Polinomial atau sepasang polinomial berdarjah tinggi, biasanya lebih daripada 3.
3. Wujud pertindihan tembereng pada gambarajah petunjuk bagi sepasang polinomial yang disekutukan.

Kaedah ini meliputi satu algoritma yang melibatkan penurunan polinomial daripada dua pembolehubah kepada satu pembolehubah sahaja. Seterusnya daripada polinomial baru yang diperolehi kita kembali kepada pemahaman poligon Newton untuk mendapatkan pensifar sepunya bagi polinomial-polinomial tersebut. Kemudian faktor penentu δ bagi anggaran di atas diperolehi. Maklumat ini kemudiannya digunakan untuk memperolehi anggaran kekardinalan di atas.

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

ON THE ESTIMATE CARDINALITY OF THE SET OF SOLUTIONS TO CONGRUENCE EQUATION BY TRANSFORMATION METHOD.

By

SHARIFAH KARTINI BINTI SAID HUSAIN

SEPTEMBER 2000

Chairman: Dr. Hj. Ismail bin Abdullah

Faculty: Science and Environmental Studies

The estimation of the cardinality of the set of solutions to congruence equation modulo a prime power p which is associated with the quartic polynomial of the form

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

in $Z_p[x,y]$ is determined by means of transformation method.

This method is utilized in certain cases or in any polynomial circumstances, that is:

1. Polynomial or a pair of non-linear polynomials.
2. Polynomial or a pair of high degree polynomials, normally exceeding 3.
3. The existence of intersection of coinciding segments in the indicator diagram of a pair of associated polynomials.

This method covers an algorithm, which involves polynomial reduction from two variables to a single variable. Consequently, from the new polynomial obtained, we return to Newton polygon in order to set common zeros for the polynomials stated. Then, the estimation of determinant factor δ is obtained. This information is later used to obtain the estimate of this cardinality.

PENGHARGAAN

Dengan nama Allah yang Maha Pemurah lagi Maha Penyayang! Kesyukuran yang tidak terhingga dirafakkan ke hadrat Ilahi kerana memberi peluang masa, usia dan ilmu untuk menyiapkan tesis ini.

Pertama sekali jutaan terima kasih diucapkan kepada Pengerusi Jawatankuasa Penyeliaan iaitu Dr. Hj. Ismail bin Abdullah atas segala kesabaran, bantuan, dorongan dan bimbingan beliau selama dua tahun yang amat bermakna.

Ribuan terima kasih juga disampaikan kepada Timbalan Naib Canselor (Akademik), Profesor Dr. Kamel Ariffin bin Mohd. Atan dan kepada Dr. Mohamad Rushdan bin Md. Said kerana dorongan dan tunjukajar yang telah mereka curahkan.

Penghargaan yang sungguh berarti buat mereka sebagai pendidik yang sentiasa bersedia mencurahkan ilmu kepada insan-insan yang dahagakan pengetahuan. Saya abadikan jasa baik mereka dalam ungkapan di bawah:

Dia
tempat berdiri tiang negara
dari keringat titisan ilmunya
mencurah menjadi benih
dalam diri
kami.

Akhir sekali saya ingin mengucapkan ribuan terima kasih kepada keluarga, terutama suami yang memahami, dan rakan-rakan yang tidak jemu memberi galakan dan semangat sehingga penulisan ini dapat disempurnakan.

Saya mengesahkan bahawa Lembaga Pemeriksa telah mengadakan peperiksaan akhir pada 30 September 2000 bagi Sharifah Kartini binti Said Husain mengenai tesis Master Sains yang bertajuk "Penganggaran Kekardinalan Bagi Set Penyelesaian Sistem Persamaan Kongruen melalui Kaedah Transformasi" mengikut Akta Universiti Pertanian Malaysia (Ijazah Lanjutan) 1980 dan Peraturan-Peraturan Universiti Pertanian Malaysia (Ijazah Lanjutan) 1981. Lembaga Pemeriksa memperakukan bahawa calon ini dianugerahkan ijazah tersebut. Ahli-ahli Lembaga Pemeriksa calon adalah seperti berikut:

HJ. HARUN BIN BUDIN, Ph.D,
Profesor Madya,
Fakulti Sains dan Pengajian Alam Sekitar,
Universiti Putra Malaysia.
(Pengerusi)

HJ. ISMAIL BIN ABDULLAH, Ph.D,
Pensyarah,
Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Putra Malaysia.
(Pemeriksa)

KAMEL ARIFFIN BIN MOHD. ATAN, Ph.D,
Profesor,
Fakulti Sains dan Pengajian Alam Sekitar,
Universiti Putra Malaysia.
(Pemeriksa)

MOHAMAD RUSHDAN BIN MD. SAID, Ph.D,
Pensyarah,
Fakulti Sains dan Pengajian Alam Sekitar,
Universiti Putra Malaysia.
(Pemeriksa)

MOHD. GHAZALI MOHAYIDIN, Ph.D,
Profesor/Timbalan Dekan Pusat Pengajian Siswazah,
Universiti Putra Malaysia.

Tarikh: 04 DEC 2000

Tesis ini telah diserahkan kepada Senat Universiti Putra Malaysia dan telah diterima sebagai memenuhi syarat keperluan untuk ijazah Master Sains.

KAMIS AWANG, Ph.D,
Profesor Madya,
Dekan Pusat Pengajian Siswazah,
Universiti Putra Malaysia.

Tarikh: 11 JAN 2001

PENGAKUAN

Saya dengan ini mengakui bahawa tesis ini adalah berdasarkan kerja saya yang asli kecuali petikan yang telah dinyatakan sumbernya. Saya juga mengakui bahawa ia tidak pernah dihantar kepada mana-mana institusi di UPM atau di tempat lain.

SHARIFAH KARTINI BINTI SAID HUSAIN

Tarikh : 25 Mei 2000

KANDUNGAN

SENARAI JADUAL

Jadual **Muka Surat**

SENARAI RAJAH

SENARAI SIMBOL DAN SINGKATAN

p	Nombor Perdana
α	Eksponen Nombor Perdana
Z	Gelanggang Integer
Q	Medan Nombor Nisbah
R	Medan Nombor Nyata
C	Medan Nombor Kompleks
Z_p	Gelanggang Integer p-adic
Q_p	Medan Nombor Nisbah p-adic
$\overline{Q_p}$	Tutupan Aljabar bagi Q_p
Ω_p	Pelengkap bagi $\overline{Q_p}$
$[a]$	Integer Terbesar yang lebih kecil atau sama dengan a
(a,b)	Pembahagi Sepunya Terbesar bagi a dan b
$\underline{x}$	n-Rangkap Pembolehubah $(x_1,\ldots,x_n)$
F	Gelanggang atau Medan
$F[x]$	Gelanggang Polinomial dengan Pekali dalam F
$\underline{f}$	m-Rangkap Polinomial $(f_1,\ldots,f_m)$, $m > 1$
$drjh\ \underline{f}$	Darjah bagi Polinomial $\underline{f}$
$J_{\underline{f}}$	Matriks Jacobian bagi $\underline{f}$
$ord_p\ a$	Kuasa Tertinggi bagi p yang membahagi a

$\nabla \underset{\sim}{f}$	Kecerunan bagi $\underset{\sim}{f}$
D	Pembezalayan
$D(\underset{\sim}{f})$	Pembezalayan bagi $\underset{\sim}{f}$
N_f	Polihedron Newton bagi f
V	Bucu pada N_f
E	Sisi pada N_f
L_f	Unjuran sisi bagi N_f
Δ	Pembezalayan
maks	Maksimum
min	Minimum
mod	Modulo
eksp	Eksponen
$\mid\ \mid_p$	Penilaian terhadap p
$\sum$	Hasil Tambah
Π	Hasil Darab
$S(f;q)$	Hasil Tambah Eksponen
$V(\underset{\sim}{f};p^{\alpha})$	Set $\{\underset{\sim}{x} \bmod p^{\alpha} : \underset{\sim}{f} \equiv \underset{\sim}{0} \bmod p^{\alpha}\}$
$N(\underset{\sim}{f};p^{\alpha})$	Kekardinalan bagi $V(\underset{\sim}{f};p^{\alpha})$

BAB 1

PENDAHULUAN

Tatatanda dan Takrifan

Lazimnya, kita tandakan Z sebagai gelanggang integer, Q sebagai medan nombor nisbah, manakala R dan C masing-masing sebagai medan nombor nyata dan medan nombor kompleks. Dengan p sentiasa menandakan nombor perdana, Q_p pula mewakili medan nombor p-adic dan Z_p gelanggang integer p-adic sementara Ω_p ialah suatu perluasan medan aljabar bagi Q_p.

Huruf kecil Roman mewakili unsur-unsur dalam Z atau Z_p. Huruf Greek α adalah sentiasa eksponen bagi suatu nombor perdana p. Simbol [ ] menandakan fungsi integer terbesar. Jika $a \in R$, maka $[a]$ akan bermakna integer terbesar yang lebih kecil atau sama dengan a. Tatatanda (a,b) menandakan pembahagi sepunya terbesar bagi a dan b, kecuali pada masa-masa tertentu yang penggunaannya jelas merujuk kepada pasangan tertib.

Tatatanda $\underline{x}$ menyatakan n-rangkap pembolehubah $(x_1, \ldots, x_n)$, dengan $n \geq 1$ dan F mewakili gelanggang atau medan, $F[\underline{x}]$ bermakna gelanggang polinomial dengan pekali dalam F. Dalam penyelidikan ini F akan merujuk sama ada kepada Z atau Q_p atau peluasan medan bagi Q_p.

Andaikan $f = \sum a_{i_1} \ldots a_{i_n} x_1^{i_1} \ldots x_n^{i_n}$ suatu polinomial dalam $F[x]$. Darjah bagi f ditakrifkan sebagai

$$\text{drjh } f = \underset{i_1 \cdots i_n}{maks}\left(i_1 + \ldots + i_n\right).$$

Simbol $\underline{f}$ bermakna m-rangkap polinomial $(f_1, \ldots, f_m)$, dengan $m \geq 1$ di dalam $F[x]$ dan $J_{\underline{f}}$ ialah matriks Jacobian $\left[\dfrac{\partial f_i}{\partial x_j}\right]$, $1 \leq i \leq m, 1 \leq j \leq n$ bagi polinomial $\underline{f}$. Andaikan $\underline{f} = (f_1, \ldots f_m)$ ialah m-rangkap polinomial linear di dalam $F[x]$. Jika $f_i = \sum a_{ij} x_j$, $1 \leq i \leq m, 1 \leq j \leq n$, kita sebut matriks $m \times n$ $[a_{ij}]$, dengan julat yang sama bagi i dan j sebagai matriks yang mewakili polinomial $\underline{f}$.

Misalkan p sebarang nombor perdana. Bagi sebarang nombor integer tak sifar a, $ord_p\, a$ menyatakan kuasa tertinggi bagi p yang membahagi a, iaitu α yang terbesar sedemikian hingga $a \equiv 0(\text{mod } p^{\alpha})$.

Jika $x = a/b$ ialah sebarang nombor nisbah, maka $ord_p\, x$ ditakrifkan sebagai $ord_p\, x = ord_p\, a - ord_p\, b$ (Suatu sifat Logaritma).

Kita mentakrifkan suatu pemetaan yang ditandakan dengan $||_p$ pada Q sebagai berikut :

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

Boleh diperlihatkan bahawa pemetaan $||_p$ seperti yang ditakrifkan di atas adalah penilaian tak-arkhimedes pada Q (Koblitz 1977).

Suatu jujukan $\{a_i\}$ yang terdiri dari nombor nisbah disebut sebagai jujukan Cauchy jika untuk suatu nombor $\xi > 0$, terdapat suatu N sedemikian hingga $|a_i - a_i'|_p < \xi$ untuk i, $i' > N$. Dua jujukan Cauchy $\{a_i\}$ dan $\{b_i\}$ dikatakan setara jika

$$\underset{i \to \infty}{had} |a_i - b_i|_p = 0.$$

Kita takrifkan medan Q_p sebagai set kelas kesetaraan jujukan Cauchy dalam Q, iaitu Q_p ialah pelengkap bagi Q terhadap penilaian $||_p$. Kita tandakan dengan $\overline{Q_p}$ sebagai tutupan bagi Q_p dan Ω_p sebagai pelengkap bagi $\overline{Q_p}$ terhadap penilaian $||_p$.

Dengan menggunakan takrifan di atas, kita dapat menyatakan takrif bagi poligon Newton bagi suatu polinomial dengan pekali dalam medan p-adic seperti yang diberikan oleh Koblitz pada tahun 1977 sebagai berikut :