



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

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

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 Kartimi 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

MUKA SURAT

DEDIKASI	ii
ABSTRAK	iii
ABSTRACT	v
PENGHARGAAN	vii
LEMBARAN PENGESAHAN	ix
PENYATAAN KEASLIAN	xi
SENARAI JADUAL	xiv
SENARAI RAJAH	xv
SENARAI SIMBOL DAN SINGKATAN	xix

BAB

I	PENGENALAN	1
	Tatatanda dan Takrifan	1
	Latar Belakang	4
	Ringkasan Keputusan	12
II	POLINOMIAL, MEDAN p-ADIC DAN POLIGON NEWTON	21
	Polinomial	21
	Gelanggang Polinomial	21
	Pensifar Polinomial	26
	Pembezalayan	30
	Medan p -adic	31
	Poligon Newton	37
III	POLIHEDRON NEWTON, GAMBARAJAH PETUNJUK DAN PERSILANGAN	
	GAMBARAJAH PETUNJUK	45
	Polihedron Newton	45
	Normal kepada Polihedron Newton	55
	Unjuran Polihedron Newton	57
	Gambarajah Petunjuk	59
	Persilangan Gambarajah Petunjuk	66
	Jenis Persilangan Gambarajah Petunjuk	67
	Persilangan Mudah	67



	Persilangan Pada Bucu	70
	Persilangan Tembereng Selari	73
	Persilangan Sepenuh	76
IV	PERINGKAT p-ADIC BAGI PENSIFAR SEPUNYA	79
	Pensifar Sepunya	79
	Peringkat p -adic bagi Pensifar Suatu Polinomial	81
	Pensifar Sepunya dan Persilangan Gambarajah Petunjuk	84
V	TRANSFORMASI	94
	Pengenalan	94
	Transformasi	96
	Langkah-langkah Transformasi	113
VI	PENYELESAIAN SISTEM PERSAMAAN KONGRUEN	147
	Hasil Tambah Eksponen	147
	Penganggaran bagi $N(f_x, f_y, p^a)$	151
	Penganggaran bagi Hasil Tambah Eksponen Berganda	155
VII	KESIMPULAN DAN CADANGAN	161
	Penemuan Utama	161
	Kesimpulan	164
	Cadangan	165
	BIBLIOGRAFI	167
	LAMPIRAN	170
	VITA	206

SENARAI JADUAL

Jadual	Muka Surat
1. Jumlah permukaan tertinggi yang terbentuk daripada sesuatu polinomial.	51

SENARAI RAJAH

Rajah	Muka Surat
1. Poligon Newton bagi $f(x) = 2x^2 - 7x - 30$ dengan $p = 2$.	39
2. Poligon Newton bagi $f(x) = 2x^3 - x^2 - x - 36$ dengan $p = 2$.	40
3. Poligon Newton bagi $f(x) = x^4 - 4/3x^3 - 26/3x^2 + 12x - 9$ dengan $p = 3$.	40
4. Gambarajah Newton bagi $f(x, y) = 2x^2 + 3xy - y^2 + 8$ dengan $p = 2$.	46
5. Gambarajah Newton bagi $f(x, y) = 9x^2 + 2xy + 9xy^2 + 27$ dengan $p = 3$.	46
6. Gambarajah Newton bagi $f(x, y) = 100x^3 + 45x^2y + 20xy^2 + 75y^3 + 125$ dengan $p = 5$.	47
7. Polihedron Newton bagi $f(x, y) = 12 + 5x + 7xy$ dengan $p = 3$.	48
8. Polihedron Newton bagi $f(x, y) = 4x^2 + 4xy^2 + y^2 - 9$ dengan $p = 3$.	49
9. Polihedron Newton bagi $f(x, y) = 9x^2 + xy + 3y^2 + 27$ dengan $p = 3$.	49
10. Polihedron Newton bagi $f(x, y) = 100x^3 + 45x^2y + 20xy^2 + 75y^3 + 125$ dengan $p = 5$.	50
11. Polihedron Newton bagi $f(x, y) = 2x^2 + 6xy + 12y^2 + 6$ dengan $p = 2$.	50
12. Unjuran L_f yang bersekutu dengan N_f bagi $f(x, y) = 12 + 5x + 7xy$ dengan $p = 2$.	58

13. Unjuran L_f yang bersekutu dengan N_f bagi
 $f(x, y) = 4x^2 + 4xy^2 + y^2 - 9$ dengan $p = 3$. 58
14. Unjuran L_f yang bersekutu dengan N_f bagi
 $f(x, y) = 100x^3 + 45x^2y + 20xy^2 + 75y^3 + 125$
dengan $p = 5$. 59
15. Gambarajah petunjuk yang bersekutu
dengan polinomial $f(x, y) = 12 + 5x + 7xy$
dengan $p = 3$. 62
16. Gambarajah petunjuk yang bersekutu
dengan polinomial $f(x, y) = 4x^2 + 4xy^2 + y^2 - 9$
dengan $p = 3$. 62
17. Gambarajah petunjuk yang bersekutu
dengan polinomial $f(x, y) = 9x^2 + xy + 3y^2 + 27$
dengan $p = 3$. 63
18. Gambarajah petunjuk yang bersekutu
dengan polinomial
 $f(x, y) = 100x^3 + 45x^2y + 20xy^2 + 75y^3 + 125$
dengan $p = 5$. 63
19. Gambarajah petunjuk yang bersekutu
dengan polinomial $f(x, y) = 2x^2 + 6xy + 12y^2 + 6$
dengan $p = 2$. 64
20. Gambarajah petunjuk bagi
 $f(x, y) = 4x + 3y + 1$ dan
 $g(x, y) = x + 14y + 6$ dengan $p = 3$. 68
21. Gambarajah petunjuk bagi
 $f(x, y) = 3x^2 + 4xy + 5$ dan
 $g(x, y) = 2x^2 + 3y^2 + 3$ dengan $p = 3$. 69
22. Gambarajah petunjuk bagi
 $f(x, y) = 3x + 2y + 5$ dan
 $g(x, y) = 4xy + 2$ dengan $p = 2$. 71

23. Gambarajah petunjuk bagi
 $f(x,y) = 3x + 2y + 5$ dan
 $g(x,y) = x + 4xy + 2$ dengan $p = 2$. 72
24. Gambarajah petunjuk bagi
 $f(x,y) = 15x^2 + 4xy + 3$ dan
 $g(x,y) = 2x^2 + 3y^2 + 4$ dengan $p = 5$. 72
25. Gambarajah petunjuk bagi
 $f(x,y) = 3x + y + 15$ dan
 $g(x,y) = 2x + 3y + 1$ dengan $p = 3$. 73
26. Gambarajah petunjuk bagi
 $f(x,y) = 3x + 9y^2 - 1$ dan
 $g(x,y) = x + 9y + 3$ dengan $p = 3$. 74
27. Gambarajah petunjuk bagi
 $f(x,y) = 4x^2 + y + 8$ dan
 $g(x,y) = 4x^2 + 3y - 2$ dengan $p = 2$. 75
28. Gambarajah petunjuk bagi
 $f(x,y) = 20x^3 + 9x^2y + 4xy^2 + 15y^3 + 25$ dan
 $g(x,y) = 3x^3 + 4x^2y + 45xy^2 + 4y^3 + 50$
dengan $p = 5$. 76
29. Gambarajah petunjuk bagi
 $f(x,y) = 12 + 5x + 7xy$ dan
 $g(x,y) = 9 + 2x^2 + 5x^2y^2$ dengan $p = 3$. 77
30. Gambarajah petunjuk bagi
 $f(x,y) = 3x + 2y + 5$ dan
 $g(x,y) = 3x + 5y + 1$ dengan $p = 3$. 78
31. Gambarajah petunjuk bagi
 $f(x,y) = 1 + 2x + 5y$ dan
 $g(x,y) = 2 + 5x + 3y$ dengan $p = 5$. 85
32. Gambarajah petunjuk bagi
 $f(x,y) = 3x + y - 15$ dan
 $g(x,y) = x + y - 9$ dengan $p = 3$. 86

33.	Gambarajah petunjuk bagi $f(x, y) = 5x + 5y - 4$ dan $g(x, y) = 3x + 3y - 8$ dengan $p = 3$.	88
34.	Gambarajah petunjuk bagi $f(x, y) = 7x + 49y^2 - 6$ dan $g(x, y) = 5x + 7y + 6$ dengan $p = 7$.	91
35.	Gambarajah petunjuk bagi $f(x, y) = x + 2y + 2$ dan $g(x, y) = 2x + 4y + 3$ dengan $p = 2$.	92
36.	Gambarajah petunjuk bagi $f(x, y) = 2 + 4x + 6y$ dan $g(x, y) = 5 + 2x + 3y$ dengan $p = 3$.	93
37.	Perubahan gambarajah petunjuk bagi g dan h .	98
38.	Gambarajah petunjuk bagi $F(U, V)$ dan $G(U, V)$.	104
39.	Gambarajah petunjuk bagi $F(U, V)$ dan $G(U, V)$.	112
40.	Gambarajah petunjuk bagi $F(U, V) = 3U^2 + 2u_0U + F_0$ dan $G(U, V) = 3V^2 + 2v_0V + G_0$ dengan $p = 2$.	117
41.	Polihedron Newton bagi $f(x, y) = 12x^2 + 4xy + y^2 + 27$ dengan $p = 3$.	120
42.	Polihedron Newton bagi $g(x, y) = 2x^2 + 2xy + 9$ dengan $p = 3$.	120
43.	Gambarajah petunjuk bagi $f(x, y) = 12x^2 + 4xy + y^2 + 27$ dan $g(x, y) = 2x^2 + 2xy + 9$ dengan $p = 3$.	121
44.	Gambarajah petunjuk bagi $F(U, V) = U^2 + 2u_0U + F_0$ dan $G(U, V) = V^2 + 2v_0V + G_0$ dengan $p = 3$.	126

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, \dots, x_n)
F	Gelanggang atau Medan
$F[x]$	Gelanggang Polinomial dengan Pekali dalam F
\underline{f}	m -Rangkap Polinomial (f_1, \dots, 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

$\nabla \underline{f}$	Kecurungan bagi \underline{f}
D	Pembezalayan
$D(\underline{f})$	Pembezalayan bagi \underline{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
$ _p$	Penilaian terhadap p
Σ	Hasil Tambah
Π	Hasil Darab
$S(f; q)$	Hasil Tambah Eksponen
$V(\underline{f}; p^\alpha)$	Set $\{ \underline{x} \bmod p^\alpha : \underline{f} \equiv \underline{0} \bmod p^\alpha \}$
$N(\underline{f}; p^\alpha)$	Kekardinalan bagi $V(\underline{f}; p^\alpha)$

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, \dots, x_n) , dengan $n \geq 1$ dan F mewakili gelanggang atau medan, $F[x]$ bermakna gelanggang

polinomial dengan pekali dalam F . Dalam penyelidikan ini F akan merujuk sama ada kepada Z atau \mathbb{Q}_p atau peluasan medan bagi \mathbb{Q}_p .

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

$$\text{drjh } f = \max_{i_1 \dots i_n} (i_1 + \dots + i_n).$$

Simbol \underline{f} bermakna m -rangkap polinomial (f_1, \dots, f_m) , dengan $m \geq 1$ di dalam $F[x]$ dan $J_{\underline{f}}$ ialah matriks Jacobian $\left[\frac{\partial f_i}{\partial x_j} \right]$, $1 \leq i \leq m, 1 \leq j \leq n$ bagi polinomial \underline{f} . Andaikan $\underline{f} = (f_1, \dots, f_m)$ 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 , $\text{ord}_p a$ menyatakan kuasa tertinggi bagi p yang membahagi a , iaitu α yang terbesar sedemikian hingga $a \equiv 0 \pmod{p^\alpha}$.

Jika $x = a/b$ ialah sebarang nombor nisbah, maka $\text{ord}_p x$ ditakrifkan sebagai $\text{ord}_p x = \text{ord}_p a - \text{ord}_p b$ (Suatu sifat Logaritma).

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

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}} & \text{jika } x \neq 0 \\ 0 & \text{jika } x = 0 \end{cases}$$

Boleh diperlihatkan bahawa pemetaan $||_p$ seperti yang ditakrifkan di atas adalah penilaian tak-arkhmedes 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 $|a_i - a_j|_p < \xi$ untuk $i, j > N$. Dua jujukan Cauchy $\{a_i\}$ dan $\{b_i\}$ dikatakan setara jika

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

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 :