TWO TOPICS IN
p-ADIC APPROXIMATION.

by

Vichian Laohakosol, B.Sc. (Hons.)(James Cook).

Thesis submitted for the degree
of Master of Science in the
Faculty of Mathematical Sciences
at the University of Adelaide.

February 1978.

Department of Pure Mathematics.

CONTENTS

CHAPTER 8: APPLICATIONS

SUMMARY

The thesis consists of two independent parts, each of which is concerned with a topic in p-adic approximation. Part 1 deals with approximation to p-adic numbers (in particular, p-adic integers) and Part 2 with approximation to p-adic functions. Since two of the most important methods of approximation to real numbers and real or complex functions are the continued fraction algorithm and interpolation, respectively, the thesis concentrates on analogues of these two methods in the p-adic context.

Part 1 is a survey and comparison of the existing different kinds of p-adic continued fractions that have been investigated so far, namely the two developed by K. Mahler [2] in 1934 as well as [4] in 1960, and the continued fraction considered by Th. Schneider [7] in 1970 and that by A. Ruban [6] in 1970. Three main aspects of these p-adic continued fractions are studied in this thesis; they are: arithmetical properties such as periodicity, metrical properties, and applications to p-adic diophantine approximations. In addition, the comparison of these p-adic continued fractions with other methods, for example, the geometrical method of K. Mahler [3] is also considered.

Part 2 is devoted to the study of p-adic interpolation for functions $f:A \rightarrow B$, where A and B are subsets of Ω_p, the completion of the algebraic closure of the field of p-adic numbers, Q_p. The theory of p-adic interpolation is developed along the lines of the exposition of Gelfond [1] in the classical case, with an emphasis on the use of divided differences and the study of analytic functions. The main tools used are the Schnirelman integral and the p-adic analogues of certain results in complex analysis. The use of the theory is illustrated by some number theoretic applications, including a simple proof of a theorem on zeros of p-adic exponential polynomials which corresponds closely to one obtained in Theorem 3 of [5] by a more complicated method by van der Poorten.

Continued :

REFERENCES

[1] GELFOND, A.O., "Calculus of finite differences", Hindustan Publishing Cooperation, 1971.

[2] MAHLER, K., "Zur Approximation p-adischer Irrationalzahlen", Nieuw Arch. Wiskunde (2), 18 (1934), 22-34.

[3] MAHLER, K., "On a geometrical representation of p-adic numbers", Ann. Math. 41 (1940), 8-56.

[4] MAHLER, K., "Lectures on diophantine approximations; Part 1: g-adic numbers and Roth's theorem", University of Notre Dame, 1960.

[5] van der POORTEN, A.J., "Hermite interpolation and p-adic exponential polynomials", J. Aust. Math. Soc. 22 (A) (1976), 12-26.

[6] RUBAN, A.A., "Certain metric properties of p-adic numbers", Sibirsk. Mat. Ž. 11 (1970), 222-227. English translation: Siberian Math. J. 11 (1970), 176-180.

[7] SCHNEIDER, Th., "Über p-adische Kettenbrüche", Symposia Math. 4 (1970), 181-189.

STATEMENT

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university and, to the best of my knowledge, contains no material previously published or written by another person, except when due reference is made in the thesis.

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude towards my supervisor, Dr. Jane Pitman, for her invaluable advice and criticisms; in particular Part 2 has been greatly improved by her advice and involves some joint work with her. (A joint paper on some results from Chapters 7 and 8 is being prepared for possible publication.)

I thank Mr. E.H. Lepp who helped translating Lutz's results in Chapter 5 and my thanks are also due to Mrs. Katherine Halsey for her excellent typing of this thesis.

GENERAL INTRODUCTION

1. The scope of the thesis.

The two topics studied in this thesis are the problem of approximation of p-adic numbers, which is dealt with in Part 1, and that of approximation of p-adic functions, which is dealt with in Part 2. The p-adic analogues of the classical continued fraction algorithm and interpolation, which are two most important and useful methods for approximating real numbers and real or complex functions, respectively, are the main methods in each part.

Part 1 surveys and compares the different kinds of p-adic continued fractions that have been investigated so far; they are the two developed by K. Mahler in [21], [25], the one developed by Th. Schneider in [37], and the one developed by A. Ruban in [34]. Two other methods for approximating p-adic numbers due to Lutz [19] and Mahler [23] are briefly discussed at the end of this part.

In Part 2, the method of p-adic interpolation is developed along the same lines as in the classical case with the aid of the Schnirelman integral. As an illustration of the method, some number theoretic results are derived in the last chapter.

The two parts are independent of each other and a detailed introduction will be provided at the beginning of each part.

2. Preliminaries and notation.

Let p denote a fixed prime, Q_p, the field of p-adic numbers, and Ω_p, the completion of its algebraic closure.

For any non-zero $\xi \in \mathcal{Q}_p$, we can write uniquely

$$\xi = c_{-m}p^{-m}+\ldots+c_{-1}p^{-1}+c_0+c_1p+\ \ldots\ ,$$

where m is an integer depending on ξ and $c_i \in \{0,1,\ldots,p-1\}$ for all i with $c_{-m} \neq 0$. The p-adic valuation, $|\cdot|_p$, of ξ is then defined by

$$|\xi|_p = p^{-m} \quad .$$

Without any confusion, $|\cdot|_p$ is also used for the extension of this valuation to Ω_p.

Throughout the whole thesis, basic properties of $\mathcal{Q}_p$ and Ω_p are assumed as given in Bachman [5] and Narici, Beckenstein and Bachman [30]. The following results in particular are basic for the whole work.

(1) For any ξ, ζ in $\mathcal{Q}_p$ or Ω_p, we have the "strong triangle inequality"

$$|\xi+\zeta|_p \leq \max\ (|\xi|_p,|\zeta|_p)\ ,$$

and this implies the "domination principle" : if $|\xi|_p < |\zeta|_p$, then

$$|\xi+\zeta|_p = |\zeta|_p\ .$$

(2) A series $\sum s_n$, with elements in $\mathcal{Q}_p$ or Ω_p, converges p-adically if and only if $|s_n|_p \to 0$ as $n \to \infty$.

(3) Let $S(\alpha,p^{-r})$ be a sphere in $\mathcal{Q}_p$ with centre α and radius $p^{-r}(r \in \mathbb{Z})$, that is

$$S(\alpha,p^{-r}) = \{\xi \in \mathcal{Q}_p;\ |\xi-\alpha|_p \leq p^{-r}\}\ .$$

Then $S(\alpha,p^{-r})$ is both open and closed. The same is true in Ω_p with $r \in \mathbb{R}$.

(4) If $S = S(\alpha,p^{-r})$ is a sphere in $\mathcal{Q}_p$, then S is compact. This is not true for spheres in Ω_p.

(5) $|\cdot|_p$ is discrete in Q_p but not in Ω_p.

(6) Let (s_n) be a sequence in Q_p. If $(|s_n|_p)$ is strictly decreasing then $|s_n|_p \to 0$ as $n \to \infty$. This is not true in Ω_p.

There are five chapters in Part 1 and three chapters in Part 2; each chapter is divided into sections numbered consecutively throughout the chapter. The major results in a given chapter are numbered consecutively throughout the chapter, regardless of whether they are called "theorem", "lemma" or "corollary", so that, for example in Chapter 1, Lemma 1.26 follows Theorem 1.25. Equations required for later reference are also numbered consecutively throughout each chapter. Definitions are either numbered as equations (for reference) or not numbered. Numbers in square brackets [ ] refer to the list of references at the end of the thesis, which combines references for both parts.

The notation set out below will be standard throughout.

p	a fixed rational prime number
$\lvert\ \rvert$	the ordinary absolute variation
$\lvert\ \rvert_p$	the p-adic valuation
Z	the ring of rational integers
Z^+	the set of positive integers (excluding 0)
Q	the field of rational numbers
R	the field of real numbers
C	the field of complex numbers
Z_p	the ring of p-adic integers
pZ_p	the set $\{p\xi;\ \xi \in Z_p\}$
Q_p	the field of p-adic numbers
Ω_p	the completion of the algebraic closure of Q_p
$S \sim T$	the set $\{s;\ s \in S \text{ and } s \notin T\}$.

PART 1

CONTINUED FRACTIONS

CHAPTER 1

INTRODUCTION AND PRELIMINARIES

This chapter will give an introduction and some background to the problem of approximation of p-adic numbers, with special emphasis on continued fractions. After a review of the basic ideas and methods of classical diophantine approximations in section 1, there will be a sketch of classical continued fractions and their applications to diophantine approximations in sections 2 and 3. Section 4 will be a brief introduction to p-adic continued fractions and p-adic diophantine approximations, and the scope of the work on these topics in this first part of the thesis will also be described in this section. Section 5 will deal with some basic results on p-adic approximation. In sections 6 and 7 we shall give some preliminaries on p-adic measure and measure preserving transformations which will be needed in Chapter 3.

In this part of the thesis, we shall be working in $\mathbb{Z}_p$ or $\mathbb{Q}_p$ and this will be clearly stated in the relevant context.

1. Basic classical ideas and methods.

The fundamental problem of classical diophantine approximation to a given real number ξ is to find good rational approximations A/B, that is, to find integers A,B such that $B \neq 0$ and

$$|\xi - A/B|$$

is small while $|B|$ is not too large. This problem leads naturally to the investigation of the forms

$$|B\xi-A| \quad \text{and} \quad |B\xi-A-\zeta|,$$

where ζ is any real number. It also leads to the problem of simultaneous approximations $A_1/B,\ldots,A_n/B$ to a system of real numbers $\xi_1,\ldots,\xi_n$ and to the study of linear forms

$$\begin{gathered}|x_1\xi_{11}+\ldots+x_n\xi_{n1}-y_1|,\\ \vdots \\ |x_1\xi_{m1}+\ldots+x_n\xi_{mn}-y_m|.\end{gathered}$$

One of the simplest results is

Dirichlet's Theorem. Let ξ be real and let $\mathcal{B}$ be a real number greater than 1. Then there exist integers A,B such that

$$0<B<\mathcal{B}, \qquad |A-B\xi| \leqslant \mathcal{B}^{-1}.$$

There are various different proofs of this theorem, all of which illustrate the basic tools available. One method is by Dirichlet's pigeon-hole principle (see for example, the first proof of Theorem 1, page 1 of Cassels [9]). Another proof is by Farey fractions (see for example Theorem 36, page 30 of Hardy and Wright [16]). A third method of proof is by using Minkowski's linear forms theorem (see for example, the second proof, page 2 of Cassels [9]), which is a simple application of a theorem in the theory of geometry of numbers. It states as follows:

Minkowski's linear forms Theorem. There are integers B_j not all 0 such that

$$\Big|\sum_{j=1}^{n}\xi_{1j}B_j\Big| \leqslant \mathcal{B}_1$$

$$\Big|\sum_{j=1}^{n}\xi_{ij}B_j\Big| < \mathcal{B}_i \qquad (2\leqslant i\leqslant n)$$

provided that

$$\mathcal{B}_1\ldots\mathcal{B}_n \geqslant |\det(\xi_{ij})|.$$

If one wants better or deeper results, more sophisticated methods are needed. One main tool available is the continued fraction algorithm which will be described in the next section. Other useful tools are those based on the geometry of numbers and analytical methods based on exponential sums.

2. Classical continued fractions.

This section is closely based on Chapter 10 of Hardy and Wright [16] and the book by Perron [31].

For each positive real number $\xi \in (0,1)$, we can write

$$\xi^{-1} = b_1 + \xi_1 ,$$

where b_1 denotes the integral part of ξ^{-1} and ξ_1 denotes the fractional part of ξ^{-1}. If $\xi_1 \neq 0$, then, since $\xi_1 < 1$, we can again write

$$\xi_1^{-1} = b_2 + \xi_2 ,$$

where now b_2 denotes the integral part of ξ_1^{-1} and ξ_2 denotes the fractional part of ξ_1^{-1}. Now repeat the procedure with ξ_2 in place of ξ_1. Continuing in this manner, we obtain a continued fraction corresponding to ξ,

$$\cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cdots}}} ,$$

which we shall write in the form

$$\frac{1}{b_1+}\ \frac{1}{b_2+}\ \frac{1}{b_3+}\ \cdots .$$

The $b_1, b_2, b_3, \ldots$ are called the partial quotients. Now put for some positive integer n,

$$A_n/B_n = \frac{1}{b_1+}\ \frac{1}{b_2+}\ \cdots\ \frac{1}{b_n} ,$$

where A_n, B_n are both positive integers and A_n/B_n is called the nth convergent to the continued fraction. The continued fraction algorithm possesses a number of interesting features, some of which will be listed below. For the proofs, see the two books just mentioned.

Theorem 1.1. If ξ, b_i $(i = 1,2,\ldots)$, A_n, B_n are as above, then

(i) $A_{-1} = 1, \quad B_{-1} = 0, \quad A_0 = 0, \quad B_0 = 1,$

$$A_{n+1} = b_n A_n + A_{n-1} \qquad (n \geqslant 1),$$

$$B_{n+1} = b_n B_n + B_{n-1};$$

(ii) $A_n B_{n-1} - A_{n-1} B_n = (-1)^{n-1} \qquad (n \geqslant 1);$

(iii) $(A_n, B_n) = 1 \qquad (n \geqslant 1),$

where (A_n, B_n) denotes the greatest common divisor of A_n and B_n;

(iv) if ξ is rational, then its continued fraction expansion is finite but if ξ is irrational, then its continued fraction is infinite and

$$A_n/B_n \to \xi \quad . \qquad (n \to \infty),$$

and in either case we therefore write

$$\xi = \frac{1}{b_1+}\ \frac{1}{b_2+}\ \frac{1}{b_3+} \cdots \quad ;$$

(v) the continued fraction of each real number ξ is unique.

As well as the simple properties mentioned above, we also have the following approximation properties.

Theorem 1.2. Let ξ be irrational and $A_n, B_n (n \geqslant 1)$ be as before. Then

$$1/B_n(B_{n+1}+B_n) < |\xi - A_n/B_n| < 1/B_n(B_n b_n + B_{n-1}) < 1/B_n^2 \; .$$

Theorem 1.3 (best approximation). Let ξ be irrational, $A_n, B_n (n>1)$ be as above. If A and B are integers such that

$$0 < B \leqslant B_n \quad \text{and} \quad A/B \neq A_n/B_n,$$

then

$$|A_n - B_n\xi| < |A - B\xi| .$$

Theorem 1.4. Let $\xi \in (0,1)$ be irrational, A_n, B_n, b_n be as before. Then

(i) of any two consecutive convergents, one at least satisfies

$$|\xi - A_n/B_n| < 1/2B_n^2 ;$$

(ii) of any three consecutive convergents, one at least satisfies

$$|\xi - A_n/B_n| < 1/\sqrt{5}\, B_n^2 ;$$

(iii) if for some $n \geqslant 2$, there is at least one b_n such that

$$b_n \geqslant 2,$$

then of any three consecutive convergents, one at least satisfies

$$|\xi - A_n/B_n| < 1/\sqrt{8}\, B_n^2 .$$

(For the proofs, see Theorems 2.14, 2.15, 2.16 pages 41-42 of Perron [31]).

Theorem 1.5. Let ξ be a real number. If A, B are two integers such that

$$|\xi - A/B| < 1/2B^2 ,$$

then A/B is a convergent to the continued fraction of ξ. (See Theorem 184 page 153 of Hardy and Wright [16] for the proof.)

One natural question concerning continued fractions is the problem of periodic continued fractions. In the classical case, it is completely answered in the following theorem (see Theorems 176, 177 pages 144-148 of Hardy and Wright [16]).

Theorem 1.6. (i) A periodic continued fraction is a quadratic surd, that is, an irrational root of a quadratic equation with rational integral coefficients.
(ii) The continued fraction which represents a quadratic surd is periodic.

Apart from the arithmetical properties described above, continued fractions also have interesting metrical properties. Most results in this direction seem to originate from the work of Khintchine (see his book [17] for discussion and proofs of the following results).

Theorem 1.7. The set of all numbers in the interval $(0,1)$ with bounded partial quotients has measure 0.

Theorem 1.8. Suppose that $(\varphi(n))$ is a sequence of positive real numbers.
(i) If $\sum_{n=1}^{\infty} 1/\varphi(n)$ diverges, then for almost all $\xi \in (0,1)$, the inequality

$$b_n = b_n(\xi) \geqslant \varphi(n)$$

holds for infinitely many n, where $b_n (n \geqslant 1)$ denotes the partial quotients of the continued fraction of ξ.
(ii) If $\sum_{n=1}^{\infty} 1/\varphi(n)$ converges, then for almost all $\xi \in (0,1)$, the above inequality holds for at most a finite number of values of n.

Theorem 1.9. There exists a positive constant B such that for almost all ξ in $(0,1)$ and for all sufficiently large n, we have

$$B_n = B_n(\xi) < \exp(Bn),$$

where B_n $(n \geqslant 1)$ are the denominators of the convergents to the continued fraction of ξ.

Theorem 1.10. For almost all ξ in $(0,1)$, we have, with the above notation,

(i) $$\lim_{n\to\infty} (b_1 b_2 \ldots b_n)^{1/n} = \prod_{k=1}^{\infty} \left(1 + \frac{1}{k^2+2k}\right)^{\log k/\log 2},$$

(ii) $$\lim_{n\to\infty} (b_1+b_2+\ldots+b_n)/n = \infty,$$

(iii) $$\lim_{n\to\infty} \log B_n/n = \pi^2/12 \log 2.$$

Theorem 1.11. (Galambos [13]). Let P be the Gauss measure defined on Lebesgue measurable subsets E of $(0,1)$ by

$$P(E) = \frac{1}{\log 2} \int_E \frac{dx}{1+x},$$

and let $b_n = b_n(\xi)$ $(n \geqslant 1)$ denote the partial quotients of the continued fraction of ξ. Then

$$\lim_{N\to\infty} P\{\xi \in (0,1);\ \max(b_1+\ldots+b_N)/N < y/\log 2\} = \exp(-1/y).$$

3. Application of contined fraction in classical diophantine approximation.

Continued fractions have been extensively applied to problems of diophantine approximation. The following theorems illustrate the kinds of result that have been obtained by this method.

<u>Theorem 1.12</u>. Let ξ be real and irrational. Then there are infinitely many positive integers B and integers A such that

$$|A-B\xi| < 1/\sqrt{5}\, B \; .$$

If ξ is of the form $\dfrac{r\cdot\frac{1}{2}(\sqrt{5}-1)+s}{t\cdot\frac{1}{2}(\sqrt{5}-1)+u}$, where $r,s,t,u \in \mathbb{Z}$ with $rs-tu = \pm 1$, the constant $1/\sqrt{5}$ cannot be replaced by any smaller number. Otherwise, there are infinitely many integers A,B with $B>0$ such that

$$|A-B\xi| < 1/\sqrt{8}\, B \; .$$

(For the proof see Theorem 5 pages 11-13 of Cassels [9]).

<u>Theorem 1.13</u> (Khintchine). To each irrational ξ, there are infinitely many integers $\mathcal{B} > 1$ such that the inequalities

$$1 \leq B \leq \mathcal{B}/2, \qquad |\xi - A/B| < 1/B\mathcal{B} \; ,$$

have no solutions in integers A,B.

(For the proof, see Theorem 24 pages 36-37 of Koksma [18]).

<u>Theorem 1.14</u> (Tchebycheff). If ξ is irrational, ζ is an arbitrary real number, then

(i) there are infinitely many integers $\mathcal{B} > 1$, A,B such that

$$|B\xi - A - \zeta| < 1/\mathcal{B} \; , \qquad |B| \leq \tfrac{1}{2}\mathcal{B} \; ,$$

(ii) there are infinitely many integers $\mathcal{B} > 1$, A,B such that

$$|B\xi - A - \zeta| < 2/\mathcal{B} \; , \qquad \tfrac{1}{2}\mathcal{B} \leq B \leq 3\mathcal{B}/2 \; .$$

(For the proof, see Theorem 2 pages 76-77 of Koksma [18]).

As an application of the metrical result (Theorem 1.8), we have:

<u>Theorem 1.15.</u> Suppose that $f(x)$ is a positive continuous function of a positive variable x and $xf(x)$ is a non-increasing function. If, for some positive c, the integral

$$\int_c^\infty f(x)\,dx$$

diverges, then the inequality

$$|\xi - A/B| < f(B)/B \qquad (B > 0)$$

has, for almost all ξ in $(0,1)$, an infinite number of solutions in integers A and B. On the other hand, if the above integral converges, then the above inequality has, for almost all ξ in $(0,1)$, only a finite number of solutions in integers A and B.
(For the proof, see Theorem 32 page 69 of Khintchine [17]).

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ as well as in $\mathbb{R}$, it is natural to investigate the approximation of elements of $\mathbb{Q}_p$ by those of $\mathbb{Q}$ and to hope that a p-adic analogue of continued fractions will yield results similar to those mentioned above.

4. <u>Continued fractions and diophantine approximation in $\mathbb{Q}_p$</u>

The study of rational approximation of p-adic numbers seems to have been initiated by K. Mahler in a series of papers starting from 1934. In his paper [20] in 1934, Mahler investigated the existence of rational integral solutions to systems of p-adic linear forms using Minkowski's linear forms theorem. In the same year, Mahler [21] developed an algorithm for constructing a p-adic continued fraction which has very good approximation properties. His method is again based on Minkowski's linear forms theorems.

Using this continued fraction, Mahler [22] in 1938 was able to prove the p-adic analogues of Theorems 1.13 and 1.14 (i) above. Since then, there have been rapid developments in many directions. In this first part of the thesis, the work will be devoted to p-adic continued fractions and results which are analogues of those obtained by continued fraction methods in the classical case as displayed in sections 2 and 3 above.

It turns out that there is no p-adic continued fraction which has all the desirable properties that the real continued fraction has. Mahler in 1961 in his book [25], which gives an excellent account of p-adic diophantine approximations, also developed another p-adic continued fraction which is closely related to the one he developed in 1934. In the last decade two more p-adic continued fractions have been studied. In 1970, Schneider [37] gave another kind of continued fraction algorithm based on the unique representation of p-adic integers as series. Also in 1970, Ruban [34]studied the p-adic continued fraction algorithm which is the most similar to the ordinary real continued fraction. The main feature of Ruban's continued fraction is the metrical properties analogous to those shown in section 2. Schneider's and Ruban's continued fractions are of the same general nature and they do not yield very good approximations; in fact Ruban's continued fraction was already mentioned by Mahler [21] but not pursued by him for this reason.

In other directions, Mahler [23] in 1940 employed a geometrical method in his study of p-adic diophantine approximation. This method yields good approximation results (mostly with good values of constants) similar to those described in section 3. Fifteen years later, Lutz [19] obtained p-adic analogues of these results as well as p-adic analogues of the metrical results discussed in section 2. Her methods are based on the geometry of numbers and the measure theory of $\mathbb{Q}_p$.

The aim of this part of the thesis is to survey all the different kinds of p-adic continued fractions referred to above and to investigate their properties and applications, as well as to compare them with one another. The remaining two sections of this chapter will indicate some preliminary methods on p-adic diophantine approximation corresponding to the classical counterpart of section 1 and also some preliminaries on p-adic measure. Chapter 2 will be concerned with p-adic continued fractions in general, and will give proofs of most of the properties common to the four p-adic continued fractions developed by Mahler, Schneider and Ruban. In Chapter 3, Ruban's and Schneider's continued fractions will be studied in detail. The two p-adic continued fractions of Mahler will be considered in Chapter 4. Finally, in Chapter 5, some applications on diophantine approximation will be illustrated and the comparison of different kinds of p-adic continued fractions will be made. A brief discussion on Mahler's geometrical method and Lutz's methods and results on p-adic diophantine approximations will also be in Chapter 5.

5. Basic p-adic tools.

While there appears to be no p-adic analogue of Farey fractions, the other two basic classical tools in section 1, namely Dirichlet's pigeon-hole principle and Minkowski's linear forms theorem, can both be applied to $\mathbb{Q}_p$. The following theorem, which is similar to results in Mahler [20], illustrates the use of both ideas.

Theorem 1.16. For given positive integers m,n, let a_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq m)$ be p-adic integers, and suppose that h_i $(1 \leq i \leq n)$ are non-negative rational integers, and let

$$h = (h_1 + h_2 + \ldots + h_n)/m \ .$$

Then there exist rational integers $x_1, \ldots, x_m$, not all 0, such that

$$\Big|\sum_{j=1}^{m} a_{ij} x_j\Big|_p \leq p^{-h_i} \qquad (i = 1, \ldots, n) \ ,$$

$$|x_j| \leq p^h \qquad (j = 1, \ldots, m) \ .$$

Proof. (i) We first use Dirichlet's pigeon-hole principle. For any rational integral point $\underset{\sim}{z}$ such that

$$|z_j| \leq p^h \qquad (j = 1, \ldots, m) \ ,$$

we may write uniquely

$$L_i(\underset{\sim}{z}) = \sum_{j=1}^{m} a_{ij} z_j = r_i(\underset{\sim}{z}) + p^{h_i}\gamma_i \qquad (i = 1, \ldots, n)$$

where $r_i(\underset{\sim}{z})$ is a rational integer such that

$$0 \leq r_i(\underset{\sim}{z}) \leq p^{h_i} - 1 \qquad (i = 1, \ldots, n) \ ,$$

and γ_i is a p-adic integer. Thus there are

$$p^{h_1 + \ldots + h_n} = p^{mh}$$

possibilities for the m-tuple $r_i(\underset{\sim}{z})$ $(i = 1, \ldots, n)$. Now the number of distinct points $\underset{\sim}{z}$ as above is

$$(2[p^h]+1)^m > p^{mh} \ ,$$

so there must be two points $\underset{\sim}{z}^{(1)}, \underset{\sim}{z}^{(2)}$, say, such that

$$r_i(\underset{\sim}{z}^{(1)}) = r_i(\underset{\sim}{z}^{(2)}) \qquad (i = 1, \ldots, n) \ .$$

It is then easily seen that $\underset{\sim}{x} = \underset{\sim}{z}^{(1)} - \underset{\sim}{z}^{(2)}$ satisfies the required inequalities.

(ii) Alternatively, as Z is dense in Z_p, it is easily seen that we may assume without loss of generality that a_{ij} are rational integers, and the theorem can then be proved by applying Minkowski's linear forms theorem to the following system of $m+n$ inequalities in $m+n$ variables $x_1,\ldots,x_n$, $R_1,\ldots,R_m$:

$$\left|\sum_{j=1}^{m} a_{ij}x_j - R_i p^{h_i}\right| < 1 \qquad (i=1,\ldots,n),$$

$$|x_j| \leqslant p^h \qquad (j=1,\ldots,m).$$

As applications of this theorem, we have the following two results, the second of which will later be the basis of one of Mahler's continued fractions.

Corollary 1.17. For given positive integers m,n, let a_{ij} $(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m)$ be p-adic integers and let h_0 be a non-negative integer. Then there exist rational integers $x_1,\ldots,x_m$, $y_1,\ldots,y_n$, not all zero, such that

$$\left|\sum_{j=1}^{m} a_{ij}x_j - y_i\right|_p \leqslant p^{-h_0} \qquad (i=1,\ldots,n),$$

$$|x_j| \leqslant p^{nh_0/(m+n)} \qquad (j=1,\ldots,m),$$

$$|y_i| \leqslant p^{nh_0/(m+n)} \qquad (i=1,\ldots,n).$$

Corollary 1.18. For a given positive integer h, let ξ be a p-adic integer. Then there are two rational integers, not both 0, such that

$$|A-B\xi|_p \leqslant p^{-h}$$

$$\max(|A|,|B|) \leqslant p^{\frac{1}{2}h} .$$

6. Preliminaries on p-adic measure theory.

We recall from the notation in the general introduction that Z_p is the set of p-adic integers, that is

$$Z_p = \{\xi \in Q_p;\ |\xi|_p \leqslant 1\} .$$

For $\xi \in Q_p$ and $r \in Z^+$, define the sphere $S(\xi,p^{-r})$ with centre ξ and radius p^{-r} by

(1,1) $\quad S(\xi,p^{-r}) = \xi + p^r Z_p = \{x \in Q_p;\ |x-\xi|_p \leqslant p^{-r}\}$.

The continued fractions of Ruban and Schneider in Chapter 3 will be defined for all ξ in pZ_p, that is for all ξ such that $|\xi|_p \leqslant p^{-1}$, and in order to obtain metrical results for these continued fractions, we shall need some results on measure in pZ_p. The first work on measure in Q_p was done by Turkstra [42] by a direct construction, and measure in Q_p can also be constructed as a Haar measure. Here we shall outline a construction using the Hahn-extension theorem and shall restrict our attention to pZ_p, though the construction easily extends to the whole of Q_p. We shall use the definitions and basic results on measure and integration of Taylor [40].

The following definitions will be used throughout all investigation on measure theory. Define

(1.2) $\quad \mathcal{S} = \{\phi\} \cup \{S(0,p^{-1})\} \cup \{S(\xi,p^{-r});$

$\qquad r \in Z^+,\ r \geqslant 2,\ \xi \in Z,\ p^{-r} < |\xi|_p \leqslant p^{-1} \text{ or } \xi = 0\}.$

(1.3) $\quad \sigma(\mathcal{S}) = \sigma\text{-field generated by } \mathcal{S}.$

We note that

$$pZ_p = S(0,p^{-1}) \in \mathcal{S} \ ;$$

and it is easily seen that if $S(\xi,p^{-r}) \in \mathcal{S}$, then

$$\xi = 0 \quad \text{or} \quad \xi = c_1p+c_2p^2+\ldots+c_{r-1}p^{r-1}$$

where $c_i \in \{0,1,\ldots,p-1\}$ for all i. It follows that $\mathcal{S}$ is countable. Clearly, we have

$$S(\xi,p^{-r}) \subseteq pZ_p \ .$$

We shall need the following results which are fundamental.

<u>Lemma 1.19</u>. Let $S(\xi,p^{-r})$ be as defined in (1.1). We have

(i) if $\beta \in S(\xi,p^{-r})$, then $S(\xi,p^{-r}) = S(\beta,p^{-r})$;

(ii) if $R = S(\xi,p^{-r})$ and $S = S(\eta,p^{-s})$ belong to $\mathcal{S}$ and $s \geqslant r$ and $R \cap S = \phi$, then $S \subseteq R$.

<u>Proof</u>. See Theorem 3 and its corollary, pages 6-7 of Narici, Beckenstein and Bachman [30].

<u>Lemma 1.20</u>. For $\mathcal{S}$ defined by (1.2), we have

(i) $\mathcal{S}$ is a semi-ring, that is,

(a) $\phi \in \mathcal{S}$,

(b) if $R,S \in \mathcal{S}$, then $R \cap S \in \mathcal{S}$,

and (c) if $R,S \in \mathcal{S}$, then, for some $n \in z^{+}$, $R \sim S = \bigcup_{i=1}^{n} S_i$, where the S_i are disjoint sets in $\mathcal{S}$.

(ii) The σ-field, $\sigma(\mathcal{S})$, is precisely the σ-field of Borel sets of pZ_p.

<u>Proof</u>. (i) follows by using the properties of spheres in Lemma 1.19 and repeatedly using the fact that

(1.4) $$Z_p = (0+pZ_p) \cup (1+pZ_p) \cup \ldots \cup \big((p-1)+pZ_p\big),$$

which is a disjoint union. (ii) follows from the fact that pZ is dense in pZ_p.

We now introduce a measure on $\mathcal{S}$, which will then be extended to $\sigma(\mathcal{S})$.

<u>Lemma 1.21</u>. Define

$$\tau : \mathcal{S} \to \mathcal{R}$$

by

$$\tau\big(S(\xi,p^{-r})\big) = p^{-r+1}, \quad \tau(\phi) = 0.$$

Then

(i) $\tau(pZ_p) = 1$,

(ii) τ is finitely additive on $\mathcal{S}$,

(iii) τ is countably additive on $\mathcal{S}$.

Proof. (i) is immediate. For (ii), we must show that if $S \in \mathcal{S}$ and $S = S_1 \cup S_2 \cup \ldots \cup S_n$, where $S_1,\ldots,S_n \in \mathcal{S}$ and are non-empty and disjoint, then

$$\tau(S) = \tau(S_1) + \tau(S_2) + \ldots + \tau(S_n).$$

Suppose $S = S(\xi,p^{-r})$ and all S_i have equal radius p^{-s}, say, and $n \geqslant 2$. Then all S_i are of the form $S(\xi_i,p^{-s})$, say. Then $s > r$ and it is easily shown that there is a unique dissection of S into p^{s-r} spheres in $\mathcal{S}$ of radius p^{-s}, so that $n = p^{s-r}$ and

$$\tau(S_1) + \ldots + \tau(S_n) = np^{-s+1} = p^{s-r}p^{-s+1} = p^{-r+1} = \tau(S),$$

as required. The general case where the radii are not all equal can then be dealt with by dissecting each of $S_1,\ldots,S_n$ into spheres in $\mathcal{S}$ of equal radius p^{-s}, say, where p^{-s} is the smallest of the radii of the S_i's. We now show (iii). Let (S_n) be a sequence of disjoint spheres such that

$$\bigcup_{n=1}^{\infty} S_n = S \in \mathcal{S}$$

Since S is compact (by (4) in section 2 of the general introduction), it follows that S has a finite subcover obtained from $\bigcup_{n=1}^{\infty} S_n$, say $\bigcup_{n=1}^{N} S_n$. Thus, for all $n > N$, $S_n = \phi$ and so $\tau(S_n) = 0$. By (ii), we have

$$\tau(S) = \sum_{n=1}^{N} \tau(S_n) = \sum_{n=1}^{\infty} \tau(S_n) ,$$

that is τ is countably additive on $\mathcal{S}$.

Lemma 1.21 immediately implies that τ is a measure on $\mathcal{S}$. Next we extend τ from $\mathcal{S}$ to $\sigma(s)$.

Theorem 1.22. There is a unique measure μ on $\sigma(s)$ such that

$$\mu|\mathcal{S} = \tau ,$$

where $\mu|S$ signifies the measure μ restricted to S and τ is as defined in Lemma 1.21.

Proof. This follows from Lemmas 1.20, 1.21 by the Hahn Extension Theorem as obtained by combining Theorems 3.4, 3.5 adn 4.2 of Taylor [40].

Theorem 1.22 yields in particular the following result.

Corollary 1.23. Let μ be as in Theorem 1.22. Suppose ρ is a measure on $\sigma(S)$ such that for all $S \in S$,

$$\rho(S) = \mu(S).$$

Then $\rho = \mu$.

From now on, let μ be the measure given by Theorem 1.22. We gather together some properties of μ which will be needed later. The proofs, which consist of straight forward checking usually based on (1.4) and Corollary 1.23, are omitted.

Theorem 1.24. Define for any $r \in Z^+$,

$$\frac{1}{1+p^r Z_p} = \left\{\frac{1}{1+p^r\alpha} \; ; \quad \alpha \in Z_p\right\}.$$

We have

(i) $\qquad 1/(1+p^r Z_p) = 1 + p^r Z_p$,

and so

$$\mu\left(1/(1+p^r Z_p)\right) = \mu(1+p^r Z_p) = p^{-r+1} ,$$

(ii) for all $\beta \in pZ_p$, $\delta \in pZ_p \sim \{0\}$,

$$1/(\delta+\beta Z_p) = (1/\delta) + (\beta/\delta^2) Z_p$$

and so

$$\mu\left(1/(1+\beta Z_p)\right) = p|\beta/\delta^2|_p ,$$

(iii) if U is the group of p-adic units, then

$$\mu(U) = \mu(1/U) = p-1 ,$$

(iv) if $\xi = c_1(\xi)p + c_2(\xi)p^2 + \ldots \in pZ_p$, where $c_i(\xi) \in \{0,1,\ldots,p-1\}$ for all i,

then for all $i \geqslant 1$,

$$\mu\{\xi \in pZ_p; c_i(\xi)=0\} = \mu\{\xi \in pZ_p; c_i(\xi)=1\} = \ldots = \mu\{\xi \in pZ_p; c_i(\xi)=p-1\} = p^{-1} .$$

For any $\alpha \in pZ_p$ and $B \in \sigma(S)$, we also have

(v) $\mu(\alpha B) = |\alpha|_p \mu(B)$,

(vi) $\mu(\alpha + B) = \mu(B)$.

7. Measure preserving transformation on pZ_p.

In this section we collect together results on measure preserving transformations needed for Chapter 3. We rely on Billingsley [8] for the basic result and we shall work in the probability space $(pZ_p, \sigma(S), \mu)$ as determined by Theorem 1.22.

A transformation

$$T : pZ_p \to pZ_p$$

is measure preserving if and only if for all $B \in \sigma(S)$,

$$\mu(T^{-1}B) = \mu(B) .$$

A set B is said to be invariant under the transformation T if and only if

$$T^{-1}B = B .$$

And define the transformation T above to be ergodic if it is measure preserving and for each invariant set B, we have

$$\mu(B) = 1 \text{ or } 0.$$

We shall be interested in ergodic transformations as they satisfy the following theorem.

Theorem 1.25 (Ergodic Theorem). Suppose T is ergodic and f is an integrable (real valued) function defined on pZ_p. Then for almost all ξ, with respect to μ, in pZ_p,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} f(T^k\xi) = \int_{pZ_p} f d\mu .$$

Proof. See Theorem 1.3 page 13 of Billingsley [8].

A stronger property which implies ergodicity is mixing. A transformation T is *mixing* if it is measure preserving and if for every pair of sets B, C in $\sigma(S)$

$$\lim_{n\to\infty} \mu(B \cap T^{-n}C) = \mu(B)\mu(C).$$

The following result will be basic for our later proofs that certain transformations are mixing.

Lemma 1.26. Let S be as in (1.2) and for $n \in Z^+$ let $S_n \subseteq S$. Suppose that for each $S \in S$, there is an $N = N(S)$ such that for $n \geqslant N$, S can be expressed as a countable (and hence, by compactness, finite) union of disjoint spheres from S_n, and also that

$$\mu(S_n \cap T^{-n}S) = \mu(S_n)\mu(S)$$

for all $S_n \in S_n$ and $n \geqslant N$. Then T is mixing and hence ergodic.

Proof. It follows easily from Theorem 1.2 of Billingsley [8]and the fact that $\sigma(S)$ is generated by the field consisting of all finite disjoint union of spheres from S that it is sufficient to prove that

$$\lim_{n\to\infty} \mu(R \cap T^{-n}S) = \mu(R)\mu(S)$$

for all $R,S \in S$. We fix $R,S \in S$ and take $n \geqslant N$, where

$$N = \max\big(N(R),N(S)\big)$$

Since $n \geqslant N(R)$, R can be expressed as a countable union of disjoing spheres in $\mathcal{S}_n$. Since the set function ν defined by

$$\nu(R) = \mu(R \cap T^{-n}S) \qquad (R \in \mathcal{S})$$

is clearly countably additive, it then follows from the definition of $N(S)$ that

$$\mu(R \cap T^{-n}S) = \mu(R)\mu(S).$$

Since this holds for all $n \geqslant N$, the required result follows.

We illustrate the above idea by a brief discussion of the "shift transformation"

$$T : pZ_p \to pZ_p ,$$

defined by

$$T : c_1p+c_2p^2 +\ldots+ c_np^n+\ldots \mapsto c_2p+c_3p^2 +\ldots+ c_np^{n-1}+\ldots$$

where $c_i \in \{0,1,\ldots,p-1\}$ for all i.

Define for $n \in Z^+$,

$$\Delta(c_1,\ldots,c_n) = c_1p+c_2p^2 +\ldots+ c_np^n+p^{n+1}Z_p .$$

Note that $\Delta(c_1,\ldots,c_n) \in \mathcal{S}$ and it is easily deduced that every sphere in $\mathcal{S}$ is a countable union of $\Delta(c_1,\ldots,c_n)$'s for sufficiently large n. Also for different c_i's, $\Delta(c_1,\ldots,c_n)$'s are disjoint. Hence by Lemma 1.26, in order to show that T is mixing, it is sufficient to prove that for sufficiently large n

$$\mu\big(\Delta(c_1,\ldots,c_n) \cap T^{-n}S\big) = \mu\big(\Delta(c_1,\ldots,c_n)\big)\mu(S) ,$$

for all $S \in \mathcal{S}$.

Clearly, fo⌊ all $S \in \mathcal{S}$,

$$\Delta(c_1,\ldots,c_n) \cap T^{-n}S = c_1p +\ldots+ c_np^n+p^nS.$$

Thus by (v) of Theorem 1.24,

$$\mu\big(\Delta(c_1,\ldots,c_n) \cap T^{-n}S\big) = p^{-n}\mu(S)$$
$$= \mu\big(\Delta(c_1,\ldots,c_n)\big)\mu(S),$$

as required.

CHAPTER 2

GENERAL p-ADIC CONTINUED FRACTIONS.

In this chapter, we shall be considering general p-adic continued fractions and some of their simple properties, most of which are common to all the p-adic continued fractions to be considered in the following two chapters. Most results obtained are straight forward analogues of classical continued fractions as in Perron [31]. Since there is no loss of generality in restricting ourselves to p-adic integers (that is, elements of Z_p), from now on the work will be carried out in Z_p unless stated otherwise. To be consistent, the following notation will be standard throughout this first part of the thesis.

1. Notation and simple properties.

The continued fractions to be considered will be of the form

$$(2.1) \qquad \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\cdots\frac{a_n}{b_n+}\cdots = \cfrac{a_0}{b_0+\cfrac{a_1}{b_1+\cfrac{a_2}{b_2+\ddots+\cfrac{a_n}{b_n+\ddots}}}}$$

where $a_i, b_i \in Q\sim\{0\}$ for all i. For any two sequences of non-zero rational numbers $a = (a_i)$, $b = (b_i)$, we define $A_n = A_n(a,b)$, $B_n = B_n(a,b)$ by

$$A_{-1} = 1, \quad B_{-1} = 0, \quad A_0 = 0, \quad B_0 = 1,$$

$$(2.2) \qquad \begin{aligned} A_{n+1} &= b_nA_n + a_nA_{n-1} \qquad (n \geq 0) \\ B_{n+1} &= b_nB_n + a_nB_{n-1}\,. \end{aligned}$$

The next theorem is a collection of simple properties that follow directly from the notation just set up. For the proofs, see Perron [31].

Theorem 2.1. Using the above notation, we have for non-zero A_n, B_n $(n \geq 1)$,

(i) $$\frac{A_n}{B_n} = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\cdots\frac{a_{n-1}}{b_{n-1}} = \frac{a_0}{B_0B_1} - \frac{a_0a_1}{B_1B_2} + \cdots + \frac{(-1)^{n-1}a_0a_1\ldots a_{n-1}}{B_{n-1}B_n} \qquad (n \geq 1),$$

(ii) $$\frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} = \frac{(-1)^{n-1}a_0a_1\ldots a_{n-1}}{B_{n-1}B_n} \qquad (n \geq 1),$$

(iii) $$\frac{A_{n+1}}{A_n} = b_n + \frac{a_n}{b_{n-1}+}\,\frac{a_{n-1}}{b_{n-2}+}\cdots\frac{a_2}{b_1} \qquad (n \geq 1),$$

$$\frac{B_{n+1}}{B_n} = b_n + \frac{a_n}{b_{n-1}+}\,\frac{a_{n-1}}{b_{n-2}+}\cdots\frac{a_1}{b_0} \qquad (n \geq 1),$$

(iv) $$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 0 \\ b_0 & 1 \end{pmatrix} \prod_{i=1}^{n-1} \begin{pmatrix} b_i & 1 \\ a_i & 0 \end{pmatrix} \qquad (n \geq 2).$$

2. Convergence.

The next natural question one may ask about the fraction (2.1) is that of its convergence. We call A_n/B_n as defined above, if it exists, the n^{th} convergent of the continued fraction (2.1) and say that the continued fraction (2.1) converges to ξ and write

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\cdots + \frac{a_n}{b_n+}\cdots$$

if and only if

$$\lim_{n\to\infty} \frac{A_n}{B_n} = \xi ,$$

where, of course, this means that

$$|\xi - A_n/B_n|_p \to 0 \qquad (n \to \infty) .$$

Writing, for non-zero A_n, B_n $(n \geq 1)$ and $A_0 = 0$, $B_0 = 1$,

$$\alpha_{n-1} = \frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} \qquad (n \geq 1),$$

it is clear that (A_n/B_n) converges p-adically if and only if

$$\alpha_n \to 0 \qquad (n \to \infty) .$$

Furthermore, by induction it can be proved that

$$\alpha_{n-1} = \frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} = \frac{(-1)^{n-1} a_0 a_1 \ldots a_{n-1}}{B_{n-1} B_n} \qquad (n \geqslant 1).$$

Hence we have proved the first part of the following theorem and the remainder is easily checked by induction.

Theorem 2.2. (i) The continued fraction

$$\frac{a_0}{b_0+} \frac{a_1}{b_1+} \cdots \frac{a_n}{b_n+} \cdots$$

converges if and only if

(2.3) $$\left| \frac{a_0 a_1 \ldots a_{n-1}}{B_{n-1} B_n} \right|_p \to 0 \qquad (n \to \infty),$$

where for all i, $a_i, b_i \in \mathcal{Q} \sim \{0\}$ and B_i are as defined in (2.2) and non-zero for $i \geqslant 0$.

(ii) Suppose the above continued fraction converges to ξ, then the continued fraction

$$b_n + \frac{a_{n+1}}{b_{n+1}+} \frac{a_{n+2}}{b_{n+2}+} \cdots$$

also converges; let the value to which it converges be ξ_n. Then for $n \geqslant 0$,

(a) $$\xi_n = b_n + \frac{a_{n+1}}{b_{n+1}+} \frac{a_{n+2}}{b_{n+2}+} \cdots ,$$

(b) $$\xi = \frac{a_0}{b_0+} \frac{a_1}{b_1+} \frac{a_2}{b_2+} \cdots = \frac{\xi_n A_n + a_n A_{n-1}}{\xi_n B_n + a_n B_{n-1}},$$

(c) $$\xi - \frac{A_n}{B_n} = \frac{(-1)^n a_0 a_1 \ldots a_n}{B_n(\xi_n B_n + a_n B_{n-1})} .$$

We shall now give some results which yield sufficient conditions for convergence in terms of the sequences $a = (a_n)$ and $b = (b_n)$.

<u>Theorem 2.3.</u> Let

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots$$

be a given continued fraction with $a_i, b_i \in \mathcal{Q} \sim \{0\}$ for all i. Suppose that

$$|b_0|_p \geq 1 \geq |a_0|_p$$

and either

(i) $$|b_i|_p > 1 \geq |a_i|_p \qquad (i \geq 1),$$

or

(ii) $$|b_i|_p \geq 1 > |a_i|_p \qquad (i \geq 1).$$

Then

(2.4) $$|B_i|_p = |b_0 b_1 \ldots b_{i-1}|_p \neq 0 \qquad (i \geq 0),$$

where for all i, B_i are as defined in (2.2) and so

(2.5) $$\left|\frac{a_0 a_1 \ldots a_{n-1}}{B_{n-1} B_n}\right|_p = \left|\frac{a_0 a_1 \ldots a_{n-1}}{b_0^2 b_1^2 \ldots b_{n-2}^2 b_{n-1}}\right|_p \qquad (n \geq 1).$$

Also the continued fraction converges to an element of Z_p.

<u>Proof</u>. Under (i) or (ii) it is immediate by induction that (2.4) holds and so (2.5) follows. Using the inequalities $|a_i/b_i|_p \leq 1/p$, we then see that

$$\left|\frac{a_0 a_1 \ldots a_{n-1}}{B_{n-1} B_n}\right|_p \to 0 \qquad (n \to \infty),$$

and hence the continued fraction converges by Theorem 2.2 (i). That the limit of convergence belongs to Z_p is evident from the facts that

$$|b_0|_p \geq |a_0|_p \ , \quad |b_i|_p > |a_i|_p \qquad (i \geq 1).$$

As seen in §2 of Chapter 1 of Perron [31], the idea of equivalent continued fractions can be used to derive a number of sufficient conditions for convergence. This same idea carries over to p-adic continued fractions. We say that two continued fractions are <u>equivalent</u> if and only if both have the same n^{th} convergents for every n. Let

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots$$

be a given continued fraction with $a_i, b_i \in \mathcal{Q} \sim \{0\}$ for all i. Let $A_n(a,b)$ and $B_n(a,b)$ be as defined in (2.2) and be non-zero for $n \geq 1$. Let also $\rho_0, \rho_1, \rho_2, \ldots$ be non-zero rational numbers. Define $A_n(\rho)$, $B_n(\rho)$ as in (2.2) but with respect to the continued fraction

$$\frac{\rho_0 a_0}{\rho_0 b_0+}\;\frac{\rho_0\rho_1 a_1}{\rho_1 b_1+}\;\frac{\rho_1\rho_2 a_2}{\rho_2 b_2+}\;\cdots$$

Then it is easily seen that for all $n \geq 0$,

$$\frac{A_n(a,b)}{B_n(a,b)} = \frac{A_n(\rho)}{B_n(\rho)},$$

and so the two continued fractions are equivalent and thus we can write

$$(2.6)\qquad \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots = \frac{\rho_0 a_0}{\rho_0 b_0+}\;\frac{\rho_0\rho_1 a_1}{\rho_1 b_1+}\;\frac{\rho_1\rho_2 a_2}{\rho_2 b_2+}\;\cdots\;\frac{\rho_{n-1}\rho_n a_n}{\rho_n b_n+}\;\cdots$$

Consequently, the convergence of one continued fraction in (2.6) implies that of the other. Upon varying values of $\rho_0, \rho_1, \rho_2, \ldots$, it is clear that different sufficient conditions for convergence can be obtained. One simple example is the following theorem.

<u>Theorem 2.4</u>. Let $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots$ be a given continued fraction with $a_i, b_i \in \mathcal{Q} \sim \{0\}$ for every i. If

$$|b_0|_p \geq 1 \geq |a_0|_p\,, \qquad |a_i|_p < |b_i b_{i-1}|_p \qquad (i \geq 1),$$

then the continued fraction converges to some ξ in Z_p.

<u>Proof</u>. Putting in (2.6),

$$\rho_i = b_i^{-1} \qquad (i \geq 0),$$

we see that

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots = \frac{b_0^{-1}a_0}{1+}\;\frac{b_0^{-1}b_1^{-1}a_1}{1+}\;\frac{b_1^{-1}b_2^{-1}a_2}{1+}\;\cdots\;.$$

Now applying Theorem 2.3 (ii) to the continued fraction on the right hand side, we see that it converges in Z_p if

$$1 > |b_{i-1}^{-1}b_i^{-1}\;a_i|_p \qquad (i \geq 1),$$

and the theorem immediately follows.

The following theorem estimates the error $\xi - (A_i/B_i)$ under the conditions of Theorem 2.4.

<u>Theorem 2.5</u>. Let $\xi \in Z_p$ have the continued fraction expansion

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots$$

where $a_i, b_i \in Q \sim \{0\}$ for all i. Let A_i, B_i be as defined in (2.2). If

$$|a_i|_p < |b_i b_{i-1}|_p \qquad (i \geq 1),$$

then

$$(2.7)\qquad \left|\xi - \frac{A_i}{B_i}\right|_p = \left|\frac{a_0a_1\ldots a_i}{B_iB_{i+1}}\right|_p = \left|\frac{a_0a_1\ldots a_i}{b_0^2b_1^2\ldots b_{i-1}^2b_i}\right|_p \qquad (i \geq 1).$$

<u>Proof</u>. From Theorem 2.1 (i), we have for $i \geq 1$,

$$\left|\xi - \frac{A_i}{B_i}\right|_p = \left|\frac{a_0a_1\ldots a_i}{B_iB_{i+1}} - \frac{a_0a_1\ldots a_{i+1}}{B_{i+1}B_{i+2}} + \cdots\right|_p .$$

Since $|a_n|_p < |b_n b_{n-i}|_p$ $(n \geq 1)$, by (2.4) of Theorem 2.3, we have

$$|B_n|_p = |b_0b_1\ldots b_{n-1}|_p \neq 0 \qquad (n \geq 0).$$

Also $|a_n|_p < |b_nb_{n-1}|_p$ $(n \geq 1)$ implies

$$\left|\frac{a_n}{b_0b_1\ldots b_{n+1}}\right|_p < \left|\frac{1}{b_0b_1\ldots b_n}\right| .$$

Combining the last two results, we get for $n \geq 1$,

$$\left|\frac{a_0a_1\ldots a_{n+1}}{b_0^2b_1^2\ldots b_n^2b_{n+1}}\right|_p = \left|\frac{a_0a_1\ldots a_{n+1}}{B_{n+2}B_{n+1}}\right|_p < \left|\frac{a_0a_1\ldots a_n}{B_nB_{n+1}}\right|_p = \left|\frac{a_0a_1\ldots a_n}{b_0^2b_1^2\ldots b_{n-1}^2b_n}\right|_p .$$

Using this last inequality and the strong triangle inequality, the theorem follows.

3. Construction of continued fraction from convergents.

If instead of directly constructing a continued fraction to a p-adic integer ξ, two sequences of non-zero rational numbers (A_n), (B_n) are given such that

$$\begin{aligned} A_{n-1}B_n - A_nB_{n-1} &\neq 0 \\ A_{n-1}B_{n+1} - A_{n+1}B_{n-1} &\neq 0 \end{aligned} \qquad (n \geqslant 0).$$

Then there is a unique pair of sequence of non-zero rational numbers $a = (a_n)$, $b = (b_n)$ such that (in the standard notation of section 1)

$$A_n = A_n(a,b), \qquad B_n = B_n(a,b) \qquad (n \geqslant -1),$$

and hence (A_n/B_n) is the sequence of convergents of the continued fraction $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots$. Moreover, if $\frac{A_n}{B_n} \to \xi$, then

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots .$$

From the idea of equivalent continued fractions, it is clear that there are infinitely many different continued fractions of which A_n/B_n are the convergents. The results just proved are summed up in the next theorem.

Theorem 2.6. Let $A_{-1} = 1$, $B_{-1} = 0$, $A_0 = 0$, $B_0 = 1$ and let (A_n), (B_n) be two sequences of non-zero rational numbers such that

$$\begin{aligned} A_{n-1}B_n - A_nB_{n-1} &\neq 0 \\ A_{n-1}B_{n+1} - A_{n+1}B_{n-1} &\neq 0 \end{aligned} \qquad (n \geqslant 0).$$

Then there exist two unique sequences of non-zero rational numbers (a_n), (b_n) satisfying

$$A_{n+1} = b_n A_n + a_n A_{n-1} \qquad (n \geq 0).$$
$$B_{n+1} = b_n B_n + a_n B_{n-1}$$

For $n \geq 0$, a_n and b_n are given uniquely by

(2.8) $$a_n = -\frac{A_n B_{n+1} - A_{n+1} B_n}{A_{n-1} B_n - A_n B_{n-1}}, \quad b_n = \frac{A_{n-1} B_{n+1} - A_{n+1} B_{n-1}}{A_{n-1} B_n - A_n B_{n-1}},$$

and (A_n/B_n) is the sequence of convergents of the continued fraction $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots$.

4. Finiteness and periodicity.

The following two theorems are almost trivial and can be proved by the same arguments as in the case of real continued fractions.

Theorem 2.7. Let $\xi \in Z_p$ have the continued fraction expansion

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\cdots\frac{a_n}{b_n},$$

where $a_i, b_i \in Q \sim \{0\}$ for $i = 0,\ldots,n$. Then $\xi \in Q$.

Definition. An infinite continued fraction $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots$ where $a_i, b_i \in Q \sim \{0\}$ for every $i \geq 0$, is said to be periodic if and only if there exist two distinct positive integers m,n such that

$$a_{m+j} = a_{m+n+j}, \quad b_{m+j} = b_{m+n+j} \qquad (j \geq 0).$$

Theorem 2.8. Let $\xi \in Z_p$ have a periodic continued fraction expansion. Then ξ satisfies a quadratic equation with rational integral coefficients.

The aim of this section is to investigate the converse results of both theorems for general p-adic continued fractions, and the approach used was suggested by Schneider [37]. The situation in the p-adic context is not entirely the same as in the classical case, for example, as will be seen in the next two chapters, there are rational numbers which have infinite p-adic continued fractions and rational numbers which have periodic continued fractions. This together with the non-uniqueness of certain continued fractions leads us to the following:

<u>Definition</u>. Let $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}$ be an infinite continued fraction with $a_i, b_i \in \mathcal{Q} \sim \{0\}$ for all i. We say that this continued fraction is <u>weakly periodic</u> if and only if there are two distinct positive integers m,n (one may be zero) such that

$$b_m + \frac{a_{m+1}}{b_{m+1}+}\,\frac{a_{m+2}}{b_{m+2}+}\,\cdots = b_n + \frac{a_{n+1}}{b_{n+1}+}\,\frac{a_{n+2}}{b_{n+2}+}\,\cdots\,.$$

We shall give a theorem that gives conditions which ensure that if ξ is a quadratic irrational and it has a continued fraction

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots \qquad (a_i, b_i \in \mathcal{Q} \sim \{0\}),$$

then this continued fraction is weakly periodic. Before doing so, however, we require some preliminary lemmas.

<u>Lemma 2.9</u> (p-adic Liouville's Theorem). Let $\xi \in Z_p$ be algebraic of degree d over $\mathcal{Q}$ and A,B be any two non-zero rational integers. Then there exists a constant k depending only on ξ and d such that

$$|\overset{B}{\cancel{b}}\xi - A|_p \geqslant kM^{-d} \quad ,$$

where $M = \max(|A|, |B|)$.

Proof. See Theorem 1 page 47 of Mahler [25].

Lemma 2.10. Let $\xi \in Z_p$ be algebraic of degree 2 over Q and let its continued fraction expansion be

$$\xi = \frac{a_0}{b_0+}\ \frac{a_1}{b_1+}\ \frac{a_2}{b_2+}\ \cdots$$

where $a_i, b_i \in Q \sim \{0\}$ for all i. Let A_n, B_n be as defined in (2.2) and non-zero for $n \geq 1$. Put

$$M_n = \max(|A_n|, |B_n|) \qquad (n \geq -1),$$

Suppose that

$$M_{n+1} > M_n \qquad (n \geq 1).$$

Then the following two statements are equivalent:

(i) there exist two constants k_1, k_2 independent of n such that

$$|B_n\xi - A_n|_p \leq k_1 M_n^{-2}, \quad M_{n+1} \leq k_2 M_n \qquad (n \geq -1),$$

(ii) there exists a constant k_3 independent of n such that

$$|B_n\xi - A_n|_p \leq k_3 M_n^{-1} M_{n+1}^{-1} \qquad (n \geq -1),$$

Proof. Suppose that (i) holds. Then (ii) is immediate. Now suppose that (ii) holds, we get by Lemma 2.9, for some k independent of n,

$$k\, M_n^{-2} \leq |B_n\xi - A_n|_p \leq k_3 M_n^{-1} M_{n+1}^{-1} \qquad (n \geq 1).$$

Thus

$$M_{n+1} \leq k_3 k^{-1} M_n \qquad (n \geq 1).$$

The cases $n = -1, 0$ are trivial from the definition. Using the hypothesis

$$M_{n+1} > M_n \qquad (n \geq 1),$$

and the definition for the cases $n = 0, -1$, the other inequality follows.

Lemma 2.11. Let the assumptions and notation be as in Lemma 2.10. Suppose that

(i) $A_n, B_n \in Z \sim \{0\}$ $(n \geq 1)$, $A_0 = 0$, $B_0 = 1$, $A_{-1} = 1$, $B_{-1} = 0$,

(ii) $M_{n+1} > M_n$ $(n \geq 0)$,

(iii) there exists a constant k_3 independent of n such that

$$|B_n\xi - A_n|_p \leq k_3 M_n^{-1} M_{n+1}^{-1} \qquad (n \geq -1),$$

(iv)
$$\Delta_n = A_{n-1}B_n - A_nB_{n-1} \neq 0 \qquad (n \geq 0),$$
$$\delta_n = A_{n-1}B_{n+1} - A_{n+1}B_{n-1} \neq 0 .$$

Then $|a_n|$, $|a_n|_p$, $|b_n|$, $|b_n|_p$ are bounded for all $n \geq 0$.

Proof. For $n \geq 0$, we have, by (2.8) of Theorem 2.6,

$$a_n = -\Delta_{n+1}/\Delta_n .$$

Thus

$$|a_n| = \left|\frac{\Delta_{n+1}}{\Delta_n}\right| \cdot \left|\frac{\Delta_n}{\Delta_n}\right|_p .$$

Now $\Delta_n \in Z \sim \{0\}$, so $|\Delta_n||\Delta_n|_p \geq 1$, and we get

$$|a_n| \leq |\Delta_{n+1}||\Delta_n|_p .$$

Clearly,

$$|\Delta_{n+1}| \leq 2M_nM_{n+1} ,$$
$$|\Delta_n|_p = |(A_{n-1}-B_{n-1}\xi)B_n-(A_n-B_n\xi)B_{n-1}|_p$$
$$\leq k_3M_{n-1}^{-1}M_n^{-1} .$$

Thus

$$|a_n| \leq 2k_3M_{n+1}M_{n-1}^{-1} \qquad (n \geq 0).$$

From Lemma 2.10, there exists a constant k_2 such that for all $n \geq 0$

$$M_{n+1} \leq k_2M_n \leq k_2^2M_{n-1} .$$

Hence, $|a_n|$ is bounded by $2k_2^2k_3$. Similarly

$$|a_n|_p \leq |\Delta_{n+1}|_p\ |\Delta_n| \leq k_3M_n^{-1}M_{n+1}^{-1} \cdot 2M_{n-1}M_n$$
$$\leq 2k_3 ,$$

using the hypothesis (ii).

As for b_n, we have for $n \geqslant 0$,

$$b_n = \delta_n/\Delta_n \ .$$

The required results follow by the same arguments as above and the facts that

$$|\delta_n| \leqslant 2M_{n-1}M_{n+1} \ ,$$

$$|\delta_n|_p = |(A_{n-1}-B_{n-1}\xi)B_{n+1} - (A_{n+1}-B_{n+1}\xi)B_{n-1}|_p$$
$$\leqslant k_3 M_{n-1}^{-1} M_n^{-1} \ .$$

Theorem 2.12. Let $\xi \in Z_p$ be a quadratic irrational having the continued fraction

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots$$

where $a_i, b_i \in Q \sim \{0\}$ for all i. Let the other notation be as in Lemma 2.10. Under the hypotheses of Lemma 2.11, the continued fraction of ξ is weakly periodic.

Proof. From Theorem 2.2 (ii)(b), we have

$$\xi = \frac{\xi_n A_n + a_n A_{n-1}}{\xi_n B_n + a_n B_{n-1}} \qquad (n \geqslant 0).$$

Let ξ satisfy the quadratic equation with integral coefficients.

$$Px^2 + Qx + R = 0 \ .$$

By substitution, we get for $n \geqslant 0$,

$$P_n\xi_n^2 + Q_n\xi_n^2 + R_n = 0 \ ,$$

where

$$P_n = PA_n^2 + QA_nB_n + RB_n^2 \ ,$$
$$Q_n = a_n\{2PA_nA_{n-1} + Q(A_nB_{n-1}+A_{n-1}B_n) + 2RB_nB_{n-1}\},$$
$$R_n = a_n^2(PA_{n-1}^2 + QA_{n-1}B_{n-1} + RB_{n-1}^2) \ .$$

We see that

$$|P_n| \leqslant c_1 M_n^2 \ ,$$

where c_1 is a constant independent of n. From the hypothesis

$$|B_n\xi - A_n|_p \leqslant k_3 M_n^{-1} M_{n+1}^{-1} < k_3 M_n^{-2} .$$

Define C_n $(n \geqslant 0)$ by

$$A_n = B_n\xi + C_n ,$$

so that

$$|C_n|_p \leqslant k_3 M_n^{-2}.$$

Eliminating A_n in the equation for P_n, we get

$$P_n = 2P\xi B_n C_n + QB_n C_n + PC_n^2 .$$

Thus

$$|P_n|_p \leqslant c_2 M_n^{-2} ,$$

where c_2 is a constant independent of n. Since P_n is an integer, then it is divisible by a high power of p, say p^{γ_n}. Thus $|P_n p^{-\gamma_n}|$ is bounded. Now consider R_n. Clearly,

$$R_n = a_n^2 P_{n-1} .$$

Using the fact that $|a_n|$ is bounded (Lemma 2.11), the estimate of $|P_{n-1}|$ and the hypothesis (ii) of Lemma 2.11, we see that there is a constant c_4 such that

$$|R_n| \leqslant c_4 M_n^2 .$$

Also using the fact that $|a_n|_p$ is bounded, the estimate of $|P_{n-1}|_p$ and the result (i) of Lemma 2.9, we see that there is a constant c_5 such that

$$|R_n|_p \leqslant c_5 M_n^{-2} .$$

Since R_n is an integer, it is also divisible by the same power of p as P_n, namely p^{γ_n} and also $|R_n p^{-\gamma_n}|$ is bounded. Now we consider Q_n. By direct computation

$$Q_n = 4P_n R_n + a_n^2 (Q^2 - 4PR)(A_n B_{n-1} - A_{n-1} B_n)^2 .$$

Using the estimates of P_n, R_n and the boundedness of $|a_n|$, $|a_n|_p$, we have

$$|Q_n| \leqslant c_6 M_n^2 ,$$
$$|Q_n|_p \leqslant c_7 M_n^{-2},$$

where c_6, c_7 are constants independent of n. By the same argument as before Q_n is divisible by $p^{\gamma n}$ and $|Q_n p^{-\gamma n}|$ is bounded. Therefore if we divide through by the common power of p in

$$P_n \xi_n^2 + Q_n \xi_n + R_n = 0,$$

we get, say,

$$X_n \xi_n^2 + Y_n \xi_n + Z_n = 0,$$

where X_n, Y_n, Z_n are integers with bounded absolute values. Therefore, there are only finitely many different triplets (X_n, Y_n, Z_n). We can then find a triplet (X, Y, Z), say, which occurs at least three times for different n. Therefore two of the corresponding roots ξ_n of the above equation must be equal at two distinct values of n say r and s. Hence

$$\xi_r = b_r + \frac{a_{r+1}}{b_{r+1}+} \frac{a_{r+2}}{b_{r+2}+} \cdots = \xi_s = b_s + \frac{a_{s+1}}{b_{s+1}+} \frac{a_{s+2}}{b_{s+2}+} \cdots ,$$

that is the continued fraction is weakly periodic.

Now we turn to the question of finiteness of continued fraction. The following theorem says roughly that to a certain extent rational numbers can not be too well approximated.

Theorem 2.13. Let $\frac{a_0}{b_0+} \frac{a_1}{b_1+} \frac{a_2}{b_2+} \cdots$ be an infinite convergent continued fraction representing an element ξ of Z_p with $a_i, b_i \in Q \sim \{0\}$ for all i and A_i, B_i are as defined in (2.2). Suppose that

(i) $A_i, B_i \in \mathbb{Z} \sim \{0\}, \quad M_{i+1} > M_i \qquad (i \geqslant 1),$

(ii) $|B_i\xi - A_i|_p < cM_i^{-2} \qquad (i \geqslant 1),$

where c is a constant independent of i and $M_i = \max(|A_i|, |B_i|)$. Then ξ is not a rational number.

Proof. Suppose on the contrary that $\xi \in \mathbb{Q}$ and let

$$\xi = r/s \quad ,$$

where r, s are integers with no common factor. By the hypotheses,

$$|B_i r - sA_i|_p < cM_i^{-2}|s|_p \leqslant cM_i^{-2} \quad (i \geqslant 1).$$

Also,

$$|B_i r - sA_i| \leqslant c'M_i \qquad (i \geqslant 1)$$

where c^1 is a constant independent of i. Thus

$$|B_i r - sA_i|_p \; |B_i r - sA_i| < cc^1 M_i^{-1} \leqslant 1,$$

for sufficiently large i. But $B_i r - sA_i$ is an integer, so we must have

$$B_i r - sA_i = 0,$$

that is $r/s = A_i/B_i$ for all large i, say $i \geqslant i(\xi)$. Writing i for $i(\xi)$ and since r and s are relatively prime, we must have

$$A_i = k_i r, \quad A_{i+1} = k_{i+1} r,$$

$$B_i = k_i s, \quad B_{i+1} = k_{i+1} s.$$

Consider for $i = i(\xi)$,

$$A_i B_{i+1} - A_{i+1} B_i = k_i k_{i+1}(rs - rs) = 0,$$

$$A_{i-1} B_i - A_i B_{i-1} \neq 0.$$

Thus from (2.8) of Theorem 2.6, we see that for $i = i(\xi)$

$$a_i = 0,$$

which contradicts the fact that $a_i \neq 0$ for every i. Hence the theorem is proved.

CHAPTER 3

THE CONTINUED FRACTIONS OF RUBAN AND SCHNEIDER

1. Introduction.

This chapter will be the investigation of two p-adic continued fractions. Sections 2 to 5 will be devoted to the one studied by Ruban in [34], [35] and [36]. As mentioned in Chaper 1, this algorithm is the most natural analogue of the classical continued fraction and had already been mentioned in Mahler [21] but not pursued because of its comparatively weak approximation properties. In fact, Ruban in [35] and [36] also extended it to a multidimensional algorithm similar to the Jacobi-Perron algorithm, but we shall restrict our attention here to the one-dimensional case. The algorithm will be developed in section 2 and by referring to Chapter 2, its basic properties will be derived in section 3. In contrast to the classical continued fraction, there are rational numbers having periodic Ruban continued fractions and this will be considered in section 4. In section 5, the measure theoretic results of sections 6 and 7 of Chapter 1 will be used to obtain metrical results for Ruban's algorithm analogous to those described in the latter part of section 2 in Chapter 1. Apart from the question of periodicity, the results obtained here are already considered in Ruban [34], but our proofs of the metrical results will rely heavily on the approach of Billingsley [8].

The remaining sections, 6 to 9, will be devoted to the closely related algorithm of Schneider in [37] and will treat this algorithm in a corresponding manner. The results in sections 6 and 7 will correspond to those in Schneider [37], but the remaining two sections on rational numbers with periodic continued fractions and on metrical results are not covered in Schneider [37].

2. Ruban continued fraction.

Without loss of generality, we restrict our consideration to numbers in pZ_p. Let $\xi \in pZ_p \sim \{0\}$ be the number whose Ruban continued fraction is to be sought. Since $\xi \neq 0$, then $|\xi^{-1}|_p > 1$ and let the unique series representation of ξ^{-1} be

$$\xi^{-1} = c_{-m}p^{-m} + c_{-m+1}p^{-m+1} + \dots + c_{-1}p^{-1} + c_0 + c_1 p + \dots ,$$

where m is a positive integer depending on ξ and $c_i \in \{0,1,\dots,p-1\}$ for all $i \geqslant -m$ with $c_{-m} \neq 0$. Define

(3.1) $$<\xi^{-1}> = c_{-m}p^{-m} + \dots + c_0 ,$$

(3.2) $$(\xi^{-1}) = c_1 p + c_2 p^2 + \dots .$$

To each ξ, $<\xi^{-1}>$ and (ξ^{-1}) are unique and so we can uniquely write

$$\xi^{-1} = <\xi^{-1}> + (\xi^{-1})$$

The algorithm proceeds as follows: write

(3.3) $$\xi^{-1} = b_0 + \xi_1 ,$$

where $b_0 = <\xi^{-1}>$, $\xi_1 = (\xi^{-1})$. If $\xi_1 = 0$, the algorithm stops. If $\xi_1 \neq 0$ and since $|\xi_1|_p < 1$, then by repeating the step just described, we can uniquely write as in (3.3),

$$\xi_1^{1} = b_1 + \xi_2 ,$$

where $b_1 = <\xi_1^{-1}>$ and $\xi_2 = (\xi_1^{-1})$ as defined in (3.1) and (3.2). Again, if $\xi_2 = 0$, the algorithm stops, otherwise it proceeds in the same manner with ξ_2 replacing ξ_1 and so on.

Since the b_i's $(i \geq 0)$ obtained are unique, then we conclude that each $\xi \in pZ_p \sim \{0\}$ has a unique Ruban continued fraction expansion of the form

$$(3,4) \qquad \frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\,\cdots$$

where b_i's are of the form $c_{-m}p^{-m}+c_{-m+1}p^{-m+1}+\ldots+c_0$ for some positive integer m and $c_i \in \{0,1,\ldots,p-1\}$ for all i, with $c_{-m} \neq 0$.

For convenience, let us define

$$(3.5) \qquad J = \{b \in Q;\ b = c_{-j}p^{-j}+c_{-j+1}p^{-j+1}+\ldots+c_0 \text{ for some } j \in Z^+,\ c_i \in \{0,1,\ldots,p-1\} \text{ for all } i,\ c_{-j} \neq 0\}.$$

We sum up and complete the above discussion inthe following theorem.

<u>Theorem 3.1</u>. To each $\xi \in pZ_p \sim \{0\}$, there corresponds a unique Ruban continued fraction $\frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\,\cdots$, where $b_i \in J$ for all i with J as defined in (3.5). This unique continued fraction converges to ξ that is

$$(3.6) \qquad \xi = \frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\,\cdots.$$

Conversely, if $b_i \in J$ for all i, then the continued fraction $\frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\,\cdots$ is a Ruban continued fraction representing a unique number ξ, say, in $pZ_p \sim \{0\}$.

<u>Proof</u>. The existence of a unique Ruban continued fraction to each $\xi \in pZ_p \sim \{0\}$ is clear from the construction. Let n be a positive integer. At the n^{th} step of construction, we have

$$\xi_{n-1}^{-1} = b_{n-1} + \xi_n\,,$$

where $b_{n-1} \in J$ and $\xi_{n-1}, \xi_n \in pZ_p$. If $\xi_n = 0$, then the continued fraction is finite and is equal to ξ. If $\xi_n \neq 0$ for every $n = Z^+$, then it can be shown by induction that

$$\xi - \frac{A_n}{B_n} = \frac{(-1)^n}{B_n(\xi_n^{-1}B_n + B_{n-1})} \qquad (n \geq 1),$$

where $\frac{A_n}{B_n} = \frac{1}{b_0+}\frac{1}{b_1+}\cdots\frac{1}{b_{n-1}}$. Since $|b_i|_p > 1$ for all $i \geq 1$, it follows from (2.4) of Theorem 2.3 that

$|B_n|_p = |b_0 b_1 \ldots b_{n-1}|_p$ and $|B_{n-1}|_p = |b_0 b_1 \ldots b_{n-2}|_p$.

Also $\xi_n \neq 0$, implies that at the $(n+1)^{th}$ step,

$$\xi_n^{-1} = b_n + \xi_{n-1} \qquad (n \geq 1),$$

with $\xi_{n+1} \in pZ_p \sim \{0\}$ and $|b_n|_p > 1$. Thus by the strong triangle inequality,

$$|\xi_n^{-1}|_p = |b_n|_p ,$$

and so

$$|\xi_n^{-1}B_n|_p = |b_0 b_1 \ldots b_n|_p > |b_0 b_1 \ldots b_{n-1}|_p = |B_{n-1}|_p .$$

Therefore, by the strong triangle inequality,

$$|\xi - A_n/B_n|_p = |b_0^2 b_1^2 \ldots b_{n-1}^2 b_n|_p^{-1} \qquad (n \geq 1),$$

and hence A_n/B_n converges to ξ. The converse is proved by using Theorem 2.3 to show convergence to some ξ and then showing that the given continued fraction must be identical with the continued fraction obtained from ξ by the Ruban algorithm.

3. Properties of Ruban continued fraction.

Ruban continued fractions possess the simple properties mentioned in (2.2), theorems 2.1, 2.2 (ii), 2.3 (i), 2.4 and 2.5. We collect here some important properties for future reference.

Theorem 3.2. Let $\xi \in pZ_p \sim \{0\}$ and let its Ruban continued fraction be

$$\xi = \frac{1}{b_0+}\frac{1}{b_1+}\frac{1}{b_2+}\cdots$$

where $b_i \in J$ for all $i \geq 0$ and J is as in (3.5). Let (A_n), (B_n) be the corresponding sequences defined by (2.2), so that the n^{th} convergent is

$$\frac{A_n}{B_n} = \frac{1}{b_0+}\,\frac{1}{b_1+}\,\cdots\,\frac{1}{b_{n-1}} \qquad (n \geq 1).$$

(i) For $n \geq 0$,

$$A_{n+1} = b_n A_n + A_{n-1}, \quad B_{n+1} = b_n B_n + B_{n-1},$$

$$|B_{n+1}|_p = |b_0 b_1 \ldots b_n|_p,$$

(ii) For $n \geq 1$,

$$\xi - \frac{A_n}{B_n} = \frac{(-1)^n}{B_n(\xi_n B_n + B_{n-1})},$$

where $\xi_n = b_n + \dfrac{1}{b_{n+1}+}\,\dfrac{1}{b_{n+2}+}\,\cdots$,

$$\left|\xi - \frac{A_n}{B_n}\right|_p = \left|\frac{1}{B_n B_{n+1}}\right|_p = \frac{1}{|b_n B_n^2|_p} = \frac{1}{|b_0^2 b_1^2 \ldots b_{n-1}^2 b_n|_p}.$$

Now let $\xi \in p\mathbb{Z}_p \sim \{0\}$ have Ruban continued fraction (3.6) and let (A_n), (B_n) be the corresponding sequences defined by (2.2). Difficulties can arise because the b_n's, A_n's, B_n's, although rational, are not necessarily integral and we overcome this problem by using the idea of equivalent continued fractions discussed in section 2 of Chapter 2. We define

(3.7)
$$\begin{aligned} \rho_n &= |b_n|_p && (n \geq 0), \\ \alpha_n &= \rho_n \rho_{n-1} && (n \geq 1), \quad \alpha_0 = \rho_0, \\ \beta_n &= \rho_n b_n && (n \geq 0), \end{aligned}$$

so that for all n, the ρ_n's are powers of p such that $\rho_n b_n \in \mathbb{Z}^+$, $|\rho_n b_n|_p = 1$, and hence

$$\alpha_n = p^{r_n}, \quad r_n \in \mathbb{Z},\ r_n \geq 0,\ \beta_n \in \mathbb{Z}^+ \qquad (n \geq 0).$$

Then by (2.6) ξ is also represented by the continued fraction

(3.8)
$$\xi = \frac{\alpha_0}{\beta_0+}\,\frac{\alpha_1}{\beta_1+}\,\frac{\alpha_2}{\beta_2+}\,\cdots.$$

In the notation of (2.2), let

(3.9) $$\mathcal{A}_n = A_n(\alpha,\beta) \;, \qquad \mathcal{B}_n = B_n(\alpha,\beta) \;.$$

Clearly, $\mathcal{A}_n \in Z^+$, $\mathcal{B}_n \in Z^+$ and by the discussion in section 2 of Chapter 2,

(3.10) $$\frac{\mathcal{A}_n}{\mathcal{B}_n} = \frac{A_n}{B_n} \;, \quad |\mathcal{B}_n|_p = 1 \qquad (n \geqslant 1).$$

Using this equivalent form, we shall give upper and lower bounds for the error $|\xi-\mathcal{A}_n/\mathcal{B}_n|_p$. First we give some preliminary results on the sizes of $\alpha_n, \beta_n, \mathcal{A}_n, \mathcal{B}_n$.

Lemma 3.3. Let $\xi \in pZ_p \sim \{0\}$ have Ruban continued fraction (3.6); (α_n), (β_n) be as in (3.7); $(\mathcal{A}_n)$, $(\mathcal{B}_n)$ be as in (3.9) and let

$$M_n = \max(|\mathcal{A}_n|, |\mathcal{B}_n|) \;.$$

Then

(i) $$1 \leqslant \beta_n \leqslant \alpha_n - 1 \qquad (n \geqslant 1),$$

(ii) $(\mathcal{A}_n)$ and $(\mathcal{B}_n)$ and hence (M_n) are strictly increasing sequences (of positive integers) and

$$(1+\alpha_n)M_{n-1} \leqslant M_{n+1} \leqslant (2\alpha_n-1)M_n \qquad (n \geqslant 1).$$

Proof. Using (3.7) and the properties of ρ_n and b_n, we get

$$\beta_n = \rho_n b_n \leqslant p\rho_n - 1 \leqslant \rho_n\rho_{n-1} - 1 = \alpha_n - 1 \quad (n \geqslant 1),$$

and this establishes (i). (ii); It follows by induction from (i) that $(\mathcal{A}_n)$ and $(\mathcal{B}_n)$ and hence (M_n) are strictly increasing. The remaining inequalities now follow by using (2.2) applied to $(\mathcal{A}_n)$ and $(\mathcal{B}_n)$.

Lemma 3.4. Let the notation be as in Lemma 3.3. Then

(i) $$M_{n+1}M_n \geqslant (1+\alpha_n)(1+\alpha_{n-1})\ldots(1+\alpha_1)\alpha_0 \;, \qquad (n \geqslant 0),$$

(ii) $$M_{n+1} < 2^n\alpha_n\alpha_{n-1}\ldots\alpha_1 \max(\alpha_0,\beta_0) \;. \qquad (n \geqslant 0).$$

Proof. We note that

$$M_2M_1 \geqslant B_2A_1 = (\beta_1\beta_0+\alpha_1)\alpha_0 = (1+\alpha_1)\alpha_0 ,$$

$$M_1M_0 \geqslant A_1B_0 = \alpha_0 .$$

Both results now follow by induction using Lemma 3.3(ii).

Theorem 3.5. Let the notation be as in Lemma 3.3. Then for $n \geqslant 1$,

(i) $$|\xi - A_n/B_n|_p = (\alpha_0\alpha_1\ldots\alpha_n)^{-1} ,$$

(ii) $$\frac{2^{n-1}}{M_n\alpha_n} > \left|\xi - \frac{A_n}{B_n}\right|_p$$

$$\geqslant \frac{(1+\alpha_1^{-1})(1+\alpha_2^{-1})\ldots(1+\alpha_n^{-1})}{M_nM_{n+1}} > \frac{1+\alpha_1^{-1}+\ldots+\alpha_n^{-1}}{M_nM_{n+1}} .$$

Proof. (i) follows directly from Theorem 2.5.
(ii) follows from (i) and Lemma 3.4.

Corollary 3.6. Let the notation be as in Lemma 3.3.

(i) If the series $\sum_{n=1}^{\infty} \frac{1}{\alpha_n}$ is divergent, there does not exist a constant k, independent of n such that

$$|\xi B_n - A_n|_p \leqslant kM_n^{-1}M_{n+1}^{-1} \qquad (n \geqslant 1).$$

(ii) If the sequence $(|\alpha_n|)$ is bounded, then there does not exist a constant k, independent of n, such that

$$|\xi B_n - A_n|_p \leqslant kM_n^{-1}M_{n+1}^{-1} \qquad (n \geqslant 1).$$

This is equivalent to saying that if there is a constant k, independent of n, satisfying

$$|\xi B_n - A_n|_p \leqslant kM_n^{-1}M_{n+1}^{-1} \qquad (n \geqslant 1),$$

then the sequence $(|\alpha_n|)$ is unbounded.

Proof. Both results follow from (3.10) that $|B_n|_p = 1$ $(n \geqslant 1)$ and Theorem 3.5.

We now look briefly at the question of periodicity. It is easily seen from uniqueness that a Ruban continued fraction is periodic if and only if it is weakly periodic in the sense of the definition given in section 4 of Chapter

2; and since Theorem 2.8 applies here, we know that if ξ has periodic Ruban continued fraction, then it satisfies a quadratic equation with rational integral coefficients, and we shall see in the next section that ξ may in fact be rational. It is easily seen that the Ruban continued fraction (3.6) is periodic if and only if the corresponding equivalent continued fraction (3.8) is periodic, and we might therefore hope to prove periodicity of the Ruban continued fractions of at least some quadratic irrationals by using Theorem 2.12, which assumes the hypotheses of Lemma 2.11. However, Corollary 3.6(ii) above shows that if ξ is a quadratic irrational in pZ_p, then the continued fraction (3.8) cannot satisfy hypothesis (iii) of Lemma 2.11 concerning the approximability of ξ, because if it did then $(|\alpha_n|)$ would be both bounded (by Lemma 2.11) and unbounded (by Corollary 3.6). Thus Theorem 2.12 gives us no information.

4. Some rational numbers with periodic Ruban continued fractions.

One remarkable property of Ruban continued fractions (3.6) is the existence of rational numbers having periodic continued fractions. For example,

$$(3.11) \qquad \frac{1}{(p-1)p^{-1}+(p-1)+}\;\frac{1}{(p-1)p^{-1}+(p-1)+}\;\frac{1}{(p-1)p^{-1}+(p-1)+}\cdots$$

is aRuban continued fraction representing the number $-p$. To see this, we solve the quadratic equation

$$px^2 + (p^2-1)x - p = 0$$

to get either $x = p^{-1}$ or $-p$. But $x \in pZ_p$, so $x = -p$. A few more examples are listed below without proofs.

(3.12) For odd primes p and $s \in \{1,2,\ldots,p-1\}$ such that s divides $(s-1)p+1$,

$$\frac{-sp}{p-1} = \frac{1}{\left((s-1)p+1\right)(sp)^{-1}+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\cdots$$

where the continued fraction on the right is periodic from the second quotient onwards.

(3.13) For $n \in Z^+$,

$$-p^n = \frac{1}{(p-1)p^{-n}+(p-1)p^{-n+1}+\ldots+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\ \frac{1}{(p-1)p^{-1}+(p-1)+}\cdots$$

where the continued fraction on the right is periodic from the second quotient onwards.

This section will be the investigation of a few cases of such continued fractions.

Period 1 : Let $\xi \in pZ_p \sim \{0\}$. Let its Ruban continued fraction be periodic with period 1, that is ξ is of the form

$$\xi = \frac{1}{b+}\ \frac{1}{b+}\ \frac{1}{b+}\ \cdots$$

where $b \in J$ (as defined in (3.5)). Then ξ satisfies the quadratic equation

$$\xi^2 + b\xi \mp 1 = 0.$$

Clearly $\xi \in Q$ if and only if $b^2 + 4$ is a perfect square. Let $m \in Z^+$ be such that $|b|_p = p^m$. Then

$$b = c_0p^{-m}+c_1p^{-m+1}+\ldots+c_{m-1}p+c_m = up^{-m}$$

where $c_i \in \{0,1,\ldots,p-1\}$ for all i with $c_{-m} \neq 0$ and $u = c_0+c_1p+\ldots+c_mp^m \in Z^+$. Therefore, $\xi \in Q$ if and only if there is an integer z satisfying

$$u^2 + 4p^{2m} = z^2 .$$

To solve this diophantine equation, write

$$4p^{2m} = (z-u)(z+u).$$

Clearly, we may suppose that $z \in Z^+$, without any loss of generality.

It is easily seen that $z-u$ and $z+u$ are both even. Hence there is an $n \in Z^+$ satisfying

$$z - u = 2n.$$

Therefore

$$p^{2m} = n(n+u) \quad .$$

Thus there are integers r,s such that $r+s = 2m$, $r > s \geq 0$ and

$$n = p^s, \quad n+u = p^r.$$

Solving for u, we get

$$u = p^s(p^{r-s}-1).$$

Since u is of the form $c_0+c_1p+\ldots+c_mp^m$ and $|u|_p = 1$, then $s = 0$, $r = 2m$ and so $u = p^{2m}-1$. But $u \leq (p-1)(1+p+\ldots+p^m) = p^{m+1}-1$, therefore $m = 0$ or 1. The case $m = 0$ is not possible because $|b|_p > 1$. Hence $m = 1$ and so

$$u = p^2 - 1 = (p-1) + (p-1)p \ .$$

Therefore, the continued fraction is (3.11), and we conclude that the only periodic Ruban continued fraction with period 1 having rational value is

$$\frac{1}{(p-1)p^{-1}+(p-1)+} \ \frac{1}{(p-1)p^{-1}+(p-1)+} \ \frac{1}{(p-1)p^{-1}+(p-1)+} \cdots = -p.$$

<u>Period 2</u> : Let $\xi \in pZ_p \sim \{0\}$ and let its periodic Ruban continued fraction be of period 2, that is ξ is of the form

$$\xi = \frac{1}{b_0+} \frac{1}{b_1+} \frac{1}{b_0+} \frac{1}{b_1+} \frac{1}{b_0+} \frac{1}{b_1+} \cdots \ .$$

We see that, as in the case of Period 1, $\xi \in \mathcal{Q}$ if and only if $(b_0b_1)^2 + 4b_0b_1$ is a perfect square. Now let

$$b_0 = c_0p^{-k}+c_1p^{-k+1}+\ldots+c_{k-1}p+c_k = u_0p^{-k} ,$$

$$b_1 = d_0p^{-K}+d_1p^{-K+1}+\ldots+d_{K-1}p+d_K = u_1p^{-K} .$$

$$\chi = k + K, \qquad u = u_0u_1 ,$$

where $k,K \in Z^+$; $c_i,d_i \in \{0,1,\ldots,p-1\}$ for all i with c_1,d_1 both $\neq 0$;

$$u_0 = c_0c_1p+\ldots+c_kp^k, \quad u_1 = d_0+d_1p+\ldots+d_Kp^K .$$

Thus, we see that $\xi \in \mathcal{Q}$ if and only if there is an integer z (which, as in the case of Period 1, we may suppose to be positive) such that

$$(u+p^{2\chi})^2 = z^2 + 4p^{2\chi} ,$$

that is,

$$4p^{2\chi} = (u+p^{2\chi}-z)(u+p^{2\chi}+z) .$$

By using the same kind of arguments as in the case of period 1 and excluding the case of Period 1, we obtain the result that there is no periodic Ruban continued fraction of (exact) period 2 having rational value.

5. Metrical properties of Ruban continued fractions.

We shall use the following notation from (1.2) and (1.3) of section 6 of Chapter 1.

$$S = \{\phi\} \cup \{S(0,p^{-1})\} \cup \{S(\xi,p^{-r}); r \in Z^+, r \geqslant 2, \xi \in Z, \\ p^{-r} < |\xi|_p \leqslant p^{-1} \text{ or } \xi = 0\},$$

$\sigma(S)$ = σ-field generated by S.

As in Chapter 1, μ denotes the measure on $\sigma(S)$ given by Theorem 1.22, or, equivalently μ is the unique Haar measure on $\sigma(S)$ normalised so that $\mu(pZ_p) = 1$.

Since our results in this section will not be affected by sets of μ-measure 0, and since $\mu(\mathcal{Q}) = 0$, we shall consider only numbers in the set

(3.14) $$I = pZ_p \sim Q\ .$$

Let $\xi \in I$ and let its Ruban continued fraction be

$$\xi = \frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\cdots\ .$$

We shall also find it convenient to use the notation

(3.15) $$\xi = \frac{1}{b_0(\xi)+}\,\frac{1}{b_1(\xi)+}\,\frac{1}{b_2(\xi)+}\cdots = [b_0(\xi),b_1(\xi),b_2(\xi),\ldots].$$

The continued fraction of ξ must be infinite since ξ is irrational (by Theorem 2.7). Define the mapping

$$T : I \to I$$

by

(3.16) $$T\xi = T\big([b_0(\xi),b_1(\xi),b_2(\xi)]\big) = [b_1(\xi),b_2(\xi),\ldots]\ .$$

where ξ is as in (3.15). The following lemma is immediate after noting that

$$T^n\xi = [b_n(\xi),b_{n+1}(\xi),b_{n+2}(\xi),\ldots] \qquad (n\geq 1).$$

<u>Lemma 3.7</u>. Let ξ be as in (3.15). Then for $n \geq 1$,

$$b_n(\xi) = b_0(T^n\xi)\ .$$

Now for fixed $b_0,b_1,\ldots b_n \in J$ (as defined in (3.5)), we define

(3.17) $$\Delta(b_0,b_1,\ldots,b_n) = \{\xi\in I; b_0(\xi)=b_0, b_1(\xi)=b_1,\ldots,b_n(\xi)=b_n\}.$$

<u>Lemma 3.8</u>. For fixed $b_0,b_1,\ldots,b_n \in J$, we have

$$\Delta(b_0,\ldots,b_n) = [b_0,\ldots,b_n] + \frac{pZ_p}{(b_0+[b_1,\ldots,b_n])^2(b_1+[b_2,\ldots,b_n])^2\cdots(b_{n-1}+[b_n])^2 b_n^2}$$

that is to say $\Delta(b_0,\ldots,b_n)$ is a sphere with centre $[b_0,\ldots,b_n]$ and radius $p^{-1}|b_0b_1\ldots b_n|_p^{-2}$.

<u>Proof</u>. The result holds for one b_i, say b_0, because

$$\Delta(b_0) = 1/(b_0+pZ_p)$$

and by Theorem 1.24(ii), this is equal to

$$\frac{1}{b_0} + \frac{pZ_p}{b_0^2} = [b_0] + \frac{pZ_p}{b_0^2} .$$

Now suppose the result holds for r b_i's and consider

$$\Delta(b_0,\ldots,b_r) = \frac{1}{b_0 + \Delta(b_1,\ldots,b_r)} .$$

By induction hypothesis,

$$\Delta(b_1,\ldots,b_r) = [b_1,\ldots,b_r]$$
$$+ \frac{pZ_p}{(b_1+[b_2,\ldots,b_r])^2(b_2+[b_3,\ldots,b_r])^2\ldots(b_{r-1}+[b_r])^2 b_r^2}$$

for which the result for $\Delta(b_0,\ldots,b_r)$ follows by another application of Theorem 1.24(ii). Thus the general result follows by induction.

Lemma 3.9. Let $S \in \mathcal{S} \cap I$. Then for all n sufficiently great S can be represented as a countable union of $\Delta(b_0,\ldots,b_n)$'s, where $\Delta(b_0,\ldots,b_n)$ is defined in (3.17).

Proof. Let $S = S(\xi, p^{-r}) \in \mathcal{S}$. For any n, each point of I belongs to some $\Delta(b_0,\ldots,b_n)$ and so $S \cap I$ can certainly be covered by $\Delta(b_0,\ldots,b_n)$'s. Moreover, by Lemma 3.8, each $\Delta(b_0,\ldots,b_n)$ is a sphere with radius less than

$$|b_0 b_1 \ldots b_n|_p^{-2} \leqslant p^{-2n-2} ,$$

and belongs to $\mathcal{S}$. We take any n such that $2n+2 \geqslant r$. Then by Lemma 1.19 (ii), each $\Delta(b_0,\ldots,b_n)$ which intersects S is completely contained in S, and so $S \cap I$ is the union of the $\Delta(b_0,\ldots,b_n)$'s which intersect it.

We now apply these results and Lemma 1.26 to prove the following theorem.

Theorem 3.10. Let T be as in (3.16). Then T is mixing and hence ergodic.

<u>Proof</u>. It is easily seen that the restriction of μ to $\{B \cap I;\ B \in \sigma(S)\}$ is determined by $\mu|S'$ where

$$S' = \{S \cap I;\ S \in S\}$$

and a slight modification of Lemma 1.26 shows that we can apply the lemma to T with S' in place of S. By Lemma 3.9, we may take S_n in Lemma 1.26 as the collection of all $\Delta(b_0,\ldots,b_{n-1})$'s. Thus, as $\mu(S \cap I) = \mu(S)$ and $T^{-n}S \cap I = T^{-n}S$, it is sufficient to prove that for each $S \in S$

$$\mu\big(\Delta(b_0,\ldots,b_{n-1}) \cap T^{-n}S\big) = \mu\big(\Delta(b_0,\ldots,b_{n-1})\big)\mu(S)$$

for all $\Delta(b_0,\ldots,b_n)$ and all n sufficiently great. From the definitions of T and $\Delta(b_0,\ldots,b_n)$, it is not difficult to see that

$$\Delta(b_0,\ldots,b_n) \cap T^{-n}S = \frac{1}{b_0+}\,\frac{1}{b_1+}\,\cdots\,\frac{1}{b_{n-1}+S}\ .$$

Now it can be shown by induction (analogous to the proof in Lemma 3.8) that

$$\frac{1}{b_0+}\,\frac{1}{b_1+}\,\cdots\,\frac{1}{b_{n-1}+S} = [b_0,\ldots,b_n] + \frac{S}{(b_0+[b_1,\ldots,b_n])^2\cdots(b_{n-1}+[b_n])^2 b_n^2}$$

and hence

$$\begin{aligned}\mu\big(\Delta(b_0,\ldots,b_{n-1}) \cap T^{-n}S\big) &= |b_0 b_1 \ldots b_n|_p^{-2}\ \mu(S)\\ &= \mu\big(\Delta(b_0,\ldots,b_n)\big)\mu(S)\ ,\end{aligned}$$

as required.

We shall now establish p-adic analogues of the metrical results in section 2 of Chapter 1 as consequences to Theorem 3.10, but first some preliminary results are required.

<u>Lemma 3.11</u>. (i) Let $b_0,b_1,\ldots,b_n \in J$ be fixed and let

$$|b_i|_p = p^{k_i} \qquad (\ i=0,\ldots,n),$$

where $k_i \in Z^+$ for all i. Then

$$\mu\{\xi \in I;\ b_0(\xi)=b_1,\ldots,b_n(\xi)=b_n\} = p^{-2k_0-2k_1-\ldots-2k_n}.$$

(ii) Let $k_0,k_1,\ldots,k_n$ be fixed positive integers. Then

$$\mu\{\xi \in I; |b_0(\xi)|_p=p^{k_0},\ldots,|b_n(\xi)|_p=p^{k_n}\} = (p-1)^n p^{-k_0-k_1-\ldots-k_n}.$$

(iii) Let $k_0,k_1,\ldots,k_n$ be fixed positive integers. Then

$$\mu\{\xi\in I; |b_0(\xi)|_p \leq p^{k_0},\ldots,|b_n(\xi)|_p \leq p^{k_n}\}$$
$$= (1-p^{-k_0})(1-p^{-k_1})\ldots(1-p^{-k_n}).$$

Proof. (i) follows easily from (3.17) and Lemma 3.8. For (ii), we note that

$$\mu\{\xi\in I; |b_0(\xi)|_p = p^{k_0},\ldots,|b_n(\xi)|_p = p^{k_n}\}$$
$$= \sum_{b_0} \cdots \sum_{b_n} \mu\{\xi\in I; b_0(\xi) = b_0,\ldots,b_n(\xi) = b_n\} ,$$

where $\sum\limits_{b_i}$ denotes the sum over all possible values of $b_i \in J$ with $|b_i|_p = p^{k_i}$ for $i = 0,\ldots,n$, and the result follows from (i). To prove (iii), we note that

$$\mu\{\xi\in I; |b_0(\xi)|_p \leq p^{k_0},\ldots,|b_n(\xi)|_p \leq p^{k_n}\}$$
$$= \sum_{i_0=1}^{k_0} \cdots \sum_{i_n=1}^{k_n} \mu\{\xi\in I; |b_0(\xi)|_p = p^{i_0},\ldots,|b_n(\xi)|_p = p^{i_n}\} ,$$

and the result follows from (ii).

Theorem 3.12. For almost all $\xi \in pZ_p$ (with respect to μ), we have

(i) $\lim\limits_{n\to\infty} |b_0(\xi)\ b_1(\xi)\ldots b_{n-1}(\xi)|_p^{1/n} = p^{p/(p-1)}$,

(ii) $\lim\limits_{n\to\infty} \frac{1}{n} \{|b_0(\xi)|_p+\ldots+|b_n(\xi)|_p\} = \infty,$

(iii) with A_n and B_n as defined in Theorem 3.2,

$$\lim_{n\to\infty} |B_{n-1}(\xi)|_p^{1/n} = \lim_{n\to\infty} |A_{n-1}(\xi)|_p^{1/n} = p^{p/(p-1)} .$$

Proof. Let T be as in (3.16). By Theorem 3.10, T is ergodic and thus satisfies the Ergodic Theorem (Theorem 1.25). Putting in the Ergodic Theorem,

$$f(\xi) = \log|b_0(\xi)|_p ,$$

and using (i) of Lemma 3.11, (i) follows. To get (ii), we take

$$f(\xi) = |b_0(\xi)|_p$$

and argue as in (i). For the first part of (iii), put

$$f(T^n\xi) = \log|B_n(\xi)/B_{n-1}(\xi)|_p \qquad (n \geqslant 1),$$

and making use of Theorem 2.1 (iii) as well as (ii) of this Theorem. For the second part of (iii), take

$$f(T^n\xi) = \log|A_n(\xi)/A_{n-1}(\xi)|_p \qquad (n \geqslant 1)$$

and argue as in the first part.

Theorem 3.13. Let ξ be as in (3.15). Then for each fixed positive integer k,

$$\mu\{\xi \in I; |b_n(\xi)|_p \leqslant p^k \text{ for all } n \geqslant 0\} = 0$$

and hence $|b_n(\xi)|_p$ is unbounded for almost all ξ in pZ_p.

Proof. This is an immediate consequence of (iii) of Lemma 3.11.

In fact, Theorem 3.13 can be further strengthened.

Theorem 3.14. Let $\varphi(n)$ be a positive-valued function defined over Z^+ such that $\sum_{n=0}^{\infty} p^{-\varphi(n)}$ diverges. Then

$$\mu\{\xi \in pZ_p; |b_n(\xi)|_p > p^{\varphi(n)} \text{ for at most a finite number of } n\} = 0.$$

Proof. The proof follows from Lemma 3.11 (iii).

The next theorem is a p-adic analogue of Theorem 1.11.

Theorem 3.15. Let $\xi \in pZ_p \sim \{0\}$ have a Ruban continued fraction (3.15). Then for any positive integer k, we have

$$\text{(i)} \quad \lim_{N\to\infty} \mu\left\{\xi \in I; \frac{\max_{0 \leqslant n \leqslant p^N-1} |b_n|_p}{p^N} \leqslant p^k\right\} = \exp(-p^{-k}) ,$$

$$\text{(ii)} \quad \lim_{N\to\infty} \mu\left\{\xi \in I; \frac{\max_{0 \leqslant n \leqslant p^N-1} |b_n|_p}{p^N} > p^k\right\} = 0.$$

Proof. From Lemma 3.11 (iii),

$$\mu\{\xi \in I;\ \max_{0\leqslant n\leqslant p^N-1} |b_n(\xi)|_p \leqslant p^{k+N}\} = (1-p^{-k-N})^{p^N} .$$

By taking limit as $N \to \infty$, (i) follows immediately.

(ii) is a direct consequence of (i).

6. Schneider continued fraction.

Let $\xi \in pZ_p \sim \{0\}$ be the number whose Schneider continued fraction is to be sought. Let the unique series expansion of ξ be

$$\xi = c_m p^m + c_{m+1} p^{m+1} + c_{m+2} p^{m+2} + \ldots ,$$

where $m \in Z^+$ is dependent on ξ and $c_i \in \{0,1,\ldots,p-1\}$ for all $i \geqslant m$ with $c_m \neq 0$. The algorithm proceeds as follows : write uniquely

$$\xi = a_0 u_0^{-1}(\xi) ,$$

where $a_0 = p^m$ and $u_0(\xi)$ is a p-adic unit. Now $u_0(\xi)$ has the unique series expansion

$$u_0(\xi) = c_{10} + c_{11} p + c_{12} p^2 + \ldots$$

where $c_{1i} \in \{0,1,\ldots,p-1\}$ for all i with $c_{10} \neq 0$. Since a_0, c_{10} are unique, then we can write

$$\xi = \frac{a_0}{b_0 + \xi_1} ,$$

where $b_0 = c_{10}$, $\xi_1 = c_{11} p + c_{12} p^2 + c_{13} p^3 + \ldots$. If $\xi_1 = 0$, the process stops. If $\xi_1 \neq 0$, let r be the smallest positive integer such that $c_{1r} \neq 0$, then we write

$$\xi_1 = a_1 u_1^{-1}(\xi) ,$$

where $a_1 = p^r$ and $u_1(\xi)$ is a p-adic unit. Now repeat the previous step with $u_0(\xi)$ replaced by $u_1(\xi)$. The algorithm continues in this manner.

Since the a_i's and b_i's obtained are unique, then ξ has a unique Schneider continued fraction

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots\,,$$

where a_i are of the form p^{r_i} with $r_i \in Z^+$ depending on ξ and $b_i \in \{1,\ldots,p-1\}$ for every i. The next theorem sums up and completes this discussion in the same way as Theorem 3.1 does for the Ruban continued fraction algorithm, and the proof, which is similar, is omitted.

Theorem 3.16. To each $\xi \in pZ_p \sim \{0\}$, there corresponds a unique Schneider continued fraction

$$\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots\,,$$

where a_i are positive powers of p and $b_i \in \{1,\ldots,p-1\}$. This unique continued fraction converges to ξ, and so

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots\,.$$

Conversely, if a_i and b_i are of the forms just mentioned, then $\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots$ is a Schneider continued fraction representing a unique number in pZ_p.

7. Properties of Schneider continued fraction.

Clearly, the Schneider continued fraction algorithm is very similar to that of Ruban. Because of this, we shall give fewer details in the derivation of its properties and omit most details. The following theorems are some of its important properties, which follow from (2.2), Theorems 2.1, 2.3 and 2.5.

Theorem 3.17. Let $\xi \in pZ_p \sim \{0\}$ and let its Schneider continued fraction be

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\cdots$$

where a_i, b_i are of the forms described in Theorem 3.16.

Let (A_n), (B_n) be the corresponding sequences defined by (2.2), so that the n^{th} convergent is

$$\frac{A_n}{B_n} = \frac{a_0}{b_0+}\ \frac{a_1}{b_1+}\ \cdots\ \frac{a_{n-1}}{b_{n-1}} \qquad (n \geqslant 1).$$

(i) For $n \geqslant 0$,

$$A_{n+1} = b_nA_n + a_nA_{n-1}, \quad B_{n+1} = b_nB_n + a_nB_{n-1},$$

$$|A_{n+1}|_p = |B_{n+1}|_p = 1.$$

(ii) For $n \geqslant 1$,

$$|\xi - A_n/B_n|_p = |a_0a_1\ldots a_n|_p = (a_0a_1\ldots a_n)^{-1}.$$

<u>Proof</u>. The only proof that needs checking is that

$$|A_{n+1}|_p = 1 \qquad (n \geqslant 0).$$

This follows easily by induction.

By similar proofs as in Theorem 3.5 and Corollary 3.6, we have also

<u>Theorem 3.18</u>. Let the notation be as in Theorem 3.17 and define

$$M_n = \max\,(|A_n|, |B_n|).$$

Then

(i) $$|\xi - A_n/B_n|_p \leqslant M_n^{-1}a_n^{-1} \qquad (n \geqslant 1),$$

(ii) $$|\xi - A_n/B_n|_p > (1+a_1^{-1}+\ldots+a_n^{-1})M_n^{-1}M_{m+1}^{-1} \qquad (n \geqslant 1),$$

(iii) if there is a constant k, independent of n, satisfying

$$|\xi - A_n/B_n|_p \leqslant k\, M_n^{-1}M_{n+1}^{-1} \qquad (n \geqslant 1),$$

then the sequence $(|a_n|)$ is unbounded.

As to the question of periodicity, similar comments to those for Ruban continued fractions, at the end of section 3, apply here also. Although Theorem 2.12 was suggested by the discussion in Schneider [37], he appears to have overlooked some points and neither Theorem 2.12 nor his discussion seems to yield information concerning continued fractions of quadratic irrationals in pZ_p.

8. Some rational numbers with periodic Schneider continued fractions.

Let us start with some examples of periodic Schneider continued fraction which can be readily verified.

(3.18)
$$\frac{p}{(p-1)+}\,\frac{p}{(p-1)+}\,\frac{p}{(p-1)+}\cdots = -p$$
$$\frac{p^r}{1+}\,\frac{p}{(p-1)+}\,\frac{p}{(p-1)+}\,\frac{p}{(p-1)+}\cdots = \frac{p^r}{1-p}$$
$$(r \in Z^+).$$

These two examples indicate the existence of periodic Schneider continued fractions possessing rational values. Similar investigations to those in section 4 will be carried out in this section.

Period 1: Let $\xi \in pZ_p \sim \{0\}$ and let its Schneider continued fraction be periodic with period 1, that is

$$\xi = \frac{a}{b+}\,\frac{a}{b+}\,\frac{a}{b+}\cdots ,$$

with $a = p^s$ for some fixed $s \in Z^+$ and $b \in \{1,\ldots,p-1\}$. With the same arguments as in section 4, we see that $\xi \in Q$ if and only if there is an integer z satisfying

$$b^2 + 4p^s = z^2 .$$

By carrying out the investigation as in section 4, we obtain the result that the only periodic Schneider continued fraction of period 1 having rational value is that in (3.18).

Period 2: Let $\xi \in pZ_p \sim \{0\}$ and let its Schneider continued fraction be periodic with period 2, that is

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\cdots ,$$

where a_0, a_1, b_0, b_1 are of the forms described in Theorem

3.16. Again by similar arguments to those of section 4, we conclude that upon excluding the case of periodic continued fractions of period 1, there is no periodic Schneider continued fractions of period 2 representing rational numbers.

9. Metrical properties of Schneider continued fraction.

Using the same notation for S, $\sigma(S)$, I as in section 5, let $\xi \in I$ and let its (infinite) Schneider continued fraction be

(3.19) $$\xi = \frac{a_0(\xi)}{b_0(\xi)+}\ \frac{a_1(\xi)}{b_1(\xi)+}\ \frac{a_2(\xi)}{b_2(\xi)+} \cdots ,$$

which we also write as

$$\xi = [a_0(\xi), a_1(\xi), \ldots ;\ b_0(\xi), b_1(\xi), \ldots].$$

Define the mapping

$$T : I \to I$$

by the rule that, for ξ as in (3.19),

(3.20) $$T\xi = \frac{a_1(\xi)}{b_1(\xi)+}\ \frac{a_2(\xi)}{b_2(\xi)+} \cdots$$

$$\xi = [a_1(\xi), a_2(\xi), \ldots ;\ b_1(\xi), b_2(\xi), \ldots]$$

Also define for any fixed $b_0, b_1, \ldots, b_n \in \{1,2,\ldots,p-1\}$ and $a_0, \ldots, a_n$ as positive powers of p

(3.21) $$\Delta(a_0,\ldots,a_n; b_0,\ldots,b_n)$$
$$= \{\xi \in I; a_0(\xi)=a_0, b_0(\xi)=b_0, \ldots, a_n(\xi)=a_n, b_n(\xi)=b_n\}.$$

Clearly, two distinct $\Delta(a_0,\ldots,a_n; b_0,\ldots,b_n)$ are disjoint.

The following three lemmas can be proved in the same way as Lemmas 3.7, 3.8, 3.9.

Lemma 3.19. Let ξ be as in (3.19) and T as in (3.20). Then

$$a_n(\xi) = a_0(T^n\xi);\ b_n(\xi) = b_0(T^n\xi) \qquad (n \geq 0).$$

Lemma 3.20. Let $a_0,\ldots,a_n,b_0,\ldots,b_n$, as before, be fixed; and let $\Delta(a_0,\ldots,a_n,b_0,\ldots,b_n)$ be as in (3.21). Then

$$\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n) = [a_0,\ldots,a_n;b_0,\ldots,b_n] + \frac{a_0a_1\ldots a_n\ pZ_p}{(b_0+[a_1,\ldots,a_n;b_1,\ldots,b_n])^2(b_1+[a_2,\ldots,a_n;b_2,\ldots,b_n])^2\ldots(b_{n-1}+[a_n;b_n])^2b_n^2}$$

Equivalently, $\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n)$ is a sphere with centre $[a_0,\ldots,a_n;b_0,\ldots,b_n]$ and radius $p^{-1}|a_0a_1\ldots a_n|_p$.

Lemma 3.21. Let S be as in section 4. For all $s \in S$, s can be represented as a countable union of $\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n)$ for all sufficiently large $n \in Z^+$.

The following theorem is proved in the same way as Theorem 3.10.

Theorem 3.22. Let T be as in (3.20). Then T is mixing and hence is ergodic.

To establish results similar to Theorem 3.12, we require the following Lemma .

Lemma 3.23. (i) Let $\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n)$ be as in (3.21) with $a_0,b_0,\ldots,a_n,b_n$ fixed. Then

$$\mu\big(\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n)\big) = |a_0a_1\ldots a_n|_p \ .$$

(ii) For fixed $s_0,s_1,\ldots,s_n \in Z^+$, we have

$$\mu\{\xi\in I; a_0(\xi)=p^{s_0},\ldots,a_n(\xi)=p^{s_n}\} = p^{-s_0-\ldots-s_n} \quad (n\geqslant 0).$$

(iii) For fixed $b_0,b_1,\ldots,b_n \in \{1,2,\ldots,p-1\}$, we have

$$\mu\{\xi\in I; b_0(\xi)=b_0,\ldots,b_n(\xi)=b_n\} = (p-1)^{-n-1} \qquad (n\geqslant 0).$$

(iv) For fixed $s_0,\ldots,s_n \in Z^+$, we have

$$\mu\{\xi\in I; a_0(\xi)\leqslant p^{s_0},\ldots,a_n(\xi)\leqslant p^{s_n}\}$$

$$= \frac{(1-p^{-s_0-1})(1-p^{-s_1-1})\ldots(1-p^{-s_n-1})}{(p-1)^{n+1}} \qquad (n\geqslant 0).$$

Proof. (i) is immediate from Lemma 3.20. To prove (ii), we note that

$$\mu\{\xi\in I; a_0(\xi)=p^{s_0},\ldots,a_n(\xi)=p^{s_n}\}$$
$$= \sum_b \mu\big(\Delta(p^{s_0},\ldots,p^{s_n};b_0,\ldots,b_n)\big) ,$$

where $\sum_b$ denotes the summation over all possible values of $b_0,\ldots,b_n$ in $\{1,2,\ldots,p-1\}$. For (iii), we note that

$$\mu\{\xi\in I; b_0(\xi)=b_0,\ldots,b_n(\xi)=b_n\} = \sum_a \mu\big(\Delta(a_0,\ldots,a_n;b_0,\ldots,b_n)\big),$$

where $\sum_a$ denotes the summation over all possible values of $a_0,\ldots,a_n$ each of which is a positive power of p. The proof of (iv) is the same as the proof of (ii) of Lemma 3.11.

With this lemma, the following theorems can be derived in much the same way as Theorems 3.12, 3.13, 3.14.

Theorem 3.24. For almost all $\xi \in pZ_p$ (with respect to μ), we have

(i) $\lim\limits_{n\to\infty} \frac{1}{n}\sum\limits_{j=0}^{n-1} a_j(\xi) = \infty,\quad \lim\limits_{n\to\infty} \frac{1}{n}\sum\limits_{j=0}^{n-1} b_j(\xi) = \frac{p}{2}$

(ii) $\lim\limits_{n\to\infty} \big(a_0(\xi)a_1(\xi)\ldots a_{n-1}(\xi)\big)^{1/n} = p^{p/(p-1)^2}$,

$\lim\limits_{n\to\infty} \big(b_0(\xi)b_1(\xi)\ldots b_{n-1}(\xi)\big)^{1/n} = \big((p-1)!\big)^{1/(p-1)}$

(iii) $\lim\limits_{n\to\infty} A_{n-1}^{1/n}(\xi) = p^{p/(p-1)^2}$, $\lim\limits_{n\to\infty} B_{n-1}^{1/n}(\xi) = \big((p-1)!\big)^{1/(p-1)}$.

Theorem 3.25. For almost all $\xi \in pZ_p$ (with respect to μ) and for any fixed positive integer k,

$$\mu\{\xi\in I; a_n(\xi) \leqslant p^k \text{ for all } n \geqslant 0\} = 0$$

and hence $a_n(\xi)$ is unbounded for almost all ξ in pZ_p.

Theorem 3.26. Let $\varphi(n)$ be a positive-valued function defined over Z^+ such that $\sum\limits_{n=0}^{\infty} p^{-\varphi(n)}$ diverges. Then

$$\mu\{\xi\in pZ_p; a_n(\xi)>p^{\varphi(n)} \text{ for at most a finite number of } n\} = 0.$$

CHAPTER 4

MAHLER CONTINUED FRACTIONS.

1. Introduction.

This chapter will be devoted to an account of the two p-adic continued fractions developed by K. Mahler. The first, developed in Mahler [21], will be referred to as Mahler I and the second, developed in Mahler [25], will be referred to as Mahler II. The construction of Mahler I and its properties will be described in sections 2 and 3. Section 4 will be the description of the algorithm of Mahler II. The last section, section 5, which is not covered by [21] and [25], will show how the two continued fractions are connected to each other.

Both Mahler I and Mahler II depend on the use of suitable approximations A/B to ξ whose existence is guaranteed by Corolloary 1.18. For convenience, we re-state the result here.

Lemma 4.1. For each p-adic integer ξ and each positive integer h, there are two rational integers not both 0 satisfying

$$(4.1)\quad \begin{cases} |A-B\xi|_p \leq p^{-h} \\ M = M(A,B) = \max(|A|,|B|) \leq p^{\frac{1}{2}h}, \end{cases}$$

and hence

$$E(A,B) = M|A-B\xi|_p \leq p^{-\frac{1}{2}h}.$$

In each case, we shall start by constructing a sequence of approximations (A_n/B_n) such that

$$A = A_n, \quad B = B_n$$

satisfy (4.1) for suitable h and satisfy further requirements. The continued fraction will then be obtained from the convergents by the process of Theorem 2.6.

2. Mahler I approximations.

Let $\xi \in Z_p \sim \{0\}$ and let

$$|\xi|_p = p^{-h(\xi)} .$$

Then we construct two sequences $(A_n),(B_n)$ of rational integers as follows.

Step 1: Apply Lemma 4.1 with

$$h = 2h(\xi) + 1 = h_1 ,$$

say. Among all the rational integral solutions of (4.1), choose a (not necessarily unique) pair

$$A = A_1, \quad B = B_1$$

for which $E(A_1,B_1)$ is least. Since $h_1 \geqslant 2h(\xi)$, it is easily checked that neither A_1 nor B_1 is 0 and the minimality of $E(A_1,B_1)$ implies that A_1 and B_1 are not simultaneously divisible by any prime other than p.

If $E(A_1,B_1) = 0$, then the process stops, otherwise proceed to

Step 2: Since $E(A_1,B_1) \leqslant p^{-1}$, there is a unique integer $h_2 > h_1$ such that

$$p^{-\frac{1}{2}h_2} < E(A_1,B_1) \leqslant p^{-\frac{1}{2}(h_2-1)} . \tag{4.2}$$

Now repeating step 1 with h_1 replaced by h_2, we obtain a pair of rational integers A_2,B_2 satisfying (4.1) and $E(A_2,B_2)$ is least among all A,B satisfying (4.1) with $h = h_2$.

If $E(A_2,B_2) = 0$, the process stops, otherwise repeat step 2 with h_2 replaced by h_3, and the algorithm continues indefinitely in this manner unless we reach an n

for which

$$E(A_n, B_n) = 0 \ ,$$

in which case it stops. It is easily seen that

(4.3) $E(A_n, B_n) = 0$ for some n if and only if $\xi \in Q$.

Hence, from now on we assume that $\xi \notin Q$ and so obtain by the algorithm infinite sequences of integers (h_n), (A_n), (B_n) and corresponding sequences (M_n), (Δ_n) defined by

$$M_n = \max(|A_n|, |B_n|) \ ,$$

$$\Delta_n = A_{n-1}B_n - A_nB_{n-1} \ ,$$

with the convention that

$$A_{-1} = 1, \ B_{-1} = 0, \ A_0 = 0, \ B_0 = 1.$$

For each n, (A_n, B_n) is thus a solution of (4.1) corresponding to $h = h_n$ for which $E(A_n, B_n)$ is least, and we have

(4.4) $$h_{n+1} > h_n \geqslant 2h(\xi) + 1 \ .$$

From the two steps of construction and the minimality of E, we have

$$E(A_1, B_1) > p^{-\frac{1}{2}h_2} \geqslant E(A_2, B_2) \ ,$$

$$M_1 \leqslant p^{\frac{1}{2}(1+2h(\xi))} < M_2 \ ,$$

and so it follows that

$$|A_1 - B_1\xi|_p > |A_2 - B_2\xi|_p \ .$$

Also

$$A_1B_2 - A_2B_1 \neq 0 \ ,$$

because otherwise $A_1/B_1 = A_2/B_2$ and since $M_1 < M_2$, there are non-zero integers f, g such that g is a power of p and

$$|f/g| > 1, \quad A_2 = A_1 f/g, \quad B_2 = B_1 f/g \ ,$$

and this implies that

$$E(A_2,B_2) = |f/g||f/g|_p \, E(A_1,B_1) \geqslant E(A_1,B_1)$$

contradicting the inequality $E(A_1,B_1) > E(A_2,B_2)$ above.

The following properties of the sequences are now easily checked by induction using the above results for $n = 1$ and 2. For $n \geqslant 1$,

$$(4.5)\quad \begin{cases} A_n \neq 0, \quad B_n \neq 0, \quad (A_n,B_n) = p^r \qquad (r \in Z^+ \cup \{0\}), \\ E(A_n,B_n) > p^{-\frac{1}{2}h_{n+1}} \geqslant E(A_{n+1},B_{n+1}), \\ M_n \leqslant p^{\frac{1}{2}h_n} < M_{n+1}, \\ |A_n - B_n\xi|_p > |A_{n+1} - B_{n+1}\xi|_p, \\ \Delta_{n+1} = A_nB_{n+1} - A_{n+1}B_n \neq 0, \quad \delta_n = A_{n-1}B_{n+1} - A_{n+1}B_{n-1} \neq 0. \end{cases}$$

From (4.5), it follows easily that for $n \geqslant 1$,

$$(4.6)\quad \begin{cases} p^{-\frac{1}{2}}M_nM_{n+1} \leqslant |\Delta_{n+1}| \leqslant 2M_nM_{n+1}, \\ \frac{1}{2}M_n^{-1}M_{n+1}^{-1} \leqslant |\Delta_{n+1}|_p \leqslant p^{\frac{1}{2}}M_n^{-1}M_{n+1}^{-1}, \\ \frac{1}{2}M_n^{-1}M_{n+1}^{-1} \leqslant |\Delta_{n+1}|_p \leqslant |A_n - B_n\xi|_p \leqslant p^{\frac{1}{2}}M_n^{-1}M_{n+1}^{-1}, \\ |A_n - B_n\xi|_p \leqslant M_n^{-2}. \end{cases}$$

Moreover, it is easily seen from (4.5) that for all n, A_n/B_n is a best approximation, that is, if A and $B \in Z$ such that $B \neq 0$ and

$$(4.7)\quad \begin{cases} |A - B\xi|_p < |A_n - B_n\xi|_p, \\ \text{then} \\ \max(|A|,|B|) > M_n. \end{cases}$$

Finally, we see from (4.5) and (4.6) that

$$(4.8)\qquad \lim_{n\to\infty} \left|\xi - \frac{A_n}{B_n}\right|_p = 0$$

and hence A_n/B_n converges (p-adically) to ξ.

3. Mahler I continued fraction.

Having obtained two sequences $(A_n),(B_n)$ of rational integers corresponding to ξ in section 2, we recall the construction described in section 3 of Chapter 2 and define two sequences of non-zero rational numbers (a_n), (b_n) by

$$(4.9)\quad \begin{aligned} a_n &= -\frac{A_nB_{n+1} - A_{n+1}B_n}{A_{n-1}B_n - A_nB_{n-1}} = -\frac{\Delta_{n+1}}{\Delta_n} \neq 0 && (n \geqslant 0) \\ b_n &= \frac{A_{n-1}B_{n+1} - A_{n+1}B_{n-1}}{A_{n-1}B_n - A_nB_{n-1}} = \frac{\delta_n}{\Delta_n} \neq 0 && (n \geqslant 0) \end{aligned}$$

with the convention

$$A_{-1} = 1,\ B_{-1} = 0,\ A_0 = 0,\ B_0 = 1.$$

The sequences $(a_n),(b_n)$ obtained are well-defined and yield a Mahler I continued fraction of ξ,

$$\xi = \frac{a_0}{b_0+}\ \frac{a_1}{b_1+}\ \frac{a_2}{b_2+}\ \cdots\quad .$$

We summarise the above discussion in the following theorem.

Theorem 4.2. Let $\xi \in Z_p$ be irrational. Then ξ has at least one (infinite) Mahler I continued fraction

$$\xi = \frac{a_0}{b_0+}\ \frac{a_1}{b_1+}\ \frac{a_2}{b_2+}\ \cdots$$

where a_n and $b_n \in Q$ for every n. The corresponding sequences $(A_n) = A(a,b)$, $(B_n) = B(a,b)$ such that A_n/B_n are the n^{th} convergents satisfy (4.5), (4.6) and (4.8) and the A_n/B_n are best approximations to ξ, that is (4.7) holds.

The next theorem indicates that the shapes of a_n and b_n as in Theorem 4.2 can be explicitly described.

Theorem 4.3. Let $\xi \in Z_p$ be irrational and let

$$\frac{a_0}{b_0+}\ \frac{a_1}{b_1+}\ \frac{a_2}{b_2+}\ \cdots$$

be a Mahler I continued fraction of ξ. Then for $n \geqslant 0$, a_n and b_n are of the forms

$$a_n = e_{n+1}p^{\alpha_n}/e_n, \quad b_n = c_n/pe_n,$$

where $\alpha_n \geqslant 0$, $c_n \neq 0$, $e_n \neq 0$, $e_{n+1} \neq 0$ are rational integers satisfying

$$|e_n| \leqslant 2\sqrt{p}, \quad |e_{n+1}| \leqslant 2\sqrt{p}, \quad |b_n| < 2\sqrt{p}|a_n| .$$

<u>Proof</u>. From (4.9), using (4.6), we obtain for $n \geqslant 0$

$$\tfrac{1}{2}p^{-\frac{1}{2}}M_{n-1}^{-1}M_{n+1} \leqslant |a_n| \leqslant 2p^{\frac{1}{2}}M_{n-1}^{-1}M_{n+1}$$

$$\tfrac{1}{2}p^{-\frac{1}{2}}M_{n-1}M_{n+1}^{-1} \leqslant |a_n|_p \leqslant 2p^{\frac{1}{2}}M_{n-1}M_{n+1}^{-1} .$$

Using (4.5), we get

$$|a_n|_p < 2,$$

and so

$$|a_n|_p \leqslant 1.$$

Therefore, a_n must be of the form

$$a_n = e_{n+1}p^{\alpha_n}/e_n ,$$

where α_n is a non-negative integer, e_n and e_{n+1} are integers not divisible by p. Now since $\Delta_n \in \mathbb{Z}$ for all n, by (4.6), we get

$$1 \leqslant |\Delta_n||\Delta_n|_p \leqslant 2\sqrt{p} \qquad (n \geqslant 0),$$

and since $a_n = -\Delta_{n+1}/\Delta_n$, then Δ_n must be of the form

$$\Delta_n = e_n p^{f_n} \qquad (n \geqslant 0),$$

where f_n is a positive integer and e_n as before is such that

$$1 \leqslant |e_n| \leqslant 2\sqrt{p} .$$

Hence, the assertion on the shape of a_n is established.

Now consider δ_n defined by

$$\delta_n = A_{n-1}B_{n+1} - A_{n+1}B_{n-1} \qquad (n \geqslant 0),$$

it is easily shown by induction that for $n \geqslant 0$,

$$p^{-\frac{1}{2}}M_{n-1}M_n \leqslant |\delta_n| \leqslant 2M_{n-1}M_{n+1} ,$$

$$\tfrac{1}{2}M_{n-1}^{-1}M_{n+1}^{-1} \leqslant |\delta_n|_p \leqslant p^{\frac{1}{2}}M_{n-1}^{-1}M_n^{-1} .$$

Therefore, from (4.9), we get for $n \geqslant 0$,

$$\tfrac{1}{2}p^{-\frac{1}{2}} \leqslant |b_n| \leqslant 2p^{\frac{1}{2}}M_n^{-1}M_{n+1} ,$$

$$\tfrac{1}{2}p^{-\frac{1}{2}}M_nM_{n+1}^{-1} \leqslant |b_n|_p \leqslant 2p^{\frac{1}{2}} \leqslant p .$$

By the same kind of arguments as in the case of a_n, we arrive at the fact that b_n must be of the form

$$b_n = c_n/pe_n \qquad (n \geqslant 0),$$

where c_n is a rational integer and e_n is as in the case of a_n. Also

$$|b_na_n^{-1}| = |\delta_n\Delta_{n+1}^{-1}| \leqslant 2p^{\frac{1}{2}}M_{n-1}M_n^{-1} ,$$

and thus

$$|b_n| < 2p^{\frac{1}{2}}|a_n| .$$

Now we turn to the question of periodic continued fractions. It is quite easily checked that all four conditions of Lemma 2.11 are always satisfied by any Mahler I continued fraction. Hence, by appealing to Theorem 2.12, we have the following theorem.

Theorem 4.4. Let $\xi \in Z_p$ be a quadratic irrational. Then any Mahler I continued fraction of ξ is weakly periodic.

We end up this section by two examples which illustrate the property that a certain part of any Mahler I continued fraction need not necessarily be a Mahler I continued fraction.

Example 4.3.1. In Q_3, $\sqrt{-2}$ exists and has a Mahler I continued fraction

$$\sqrt{-2} = \frac{1}{1+}\,\frac{6}{-5+}\,\frac{9/2}{-\frac{1}{2}+}\,\frac{3}{-2+}\,\frac{-3}{2+}\,\frac{3}{-2+}\,\cdots\;.$$

Consider the number

$$\zeta = \frac{6}{-5+}\,\frac{9/2}{-\frac{1}{2}+}\,\frac{3}{-2+}\,\frac{-3}{2+}\,\frac{3}{-2+}\,\cdots$$

$$= 2.3 + 3^2u\;,$$

where u is a p-adic unit depending on ζ. Any Mahler I continued fraction of ζ is of the form

$$\zeta = \frac{-3}{1+}\,\cdots$$

which is not the same as $\frac{6}{-5+}\,\frac{9/2}{-\frac{1}{2}+}\,\frac{3}{-2+}\,\frac{-3}{2+}\,\frac{3}{-2+}\,\cdots$.

Example 4.3.2. In $\mathbb{Q}_5$, $\sqrt{-1}$ exists and has a Mahler I continued fraction

$$\sqrt{-1} = \frac{-1}{2+}\,\frac{10}{-3+}\,\frac{5/2}{3/2+}\,\frac{-5}{4+}\,\frac{10}{-3+}\,\cdots\;.$$

Consider the number

$$\zeta = \frac{10}{-3+}\,\frac{5/2}{3/2+}\,\frac{-5}{4+}\,\frac{10}{-3+}\,\cdots$$

$$= 1.5 + 5^2u$$

where u is a p-adic unit depending on ζ. Any Mahler I continued fraction of ζ is of the form

$$\zeta = \frac{5}{1+}\,\cdots$$

which is not the same as $\frac{10}{-3+}\,\frac{5/2}{3/2+}\,\frac{-5}{4+}\,\frac{10}{-3+}\,\cdots$

4. Mahler II approximations and continued fraction.

The Mahler II continued fraction depends on an explicit method for solving (4.1), which we now describe.

For any given irrational $\xi \in Z_p$, write

$$\xi = c_0 + c_1p + c_2p^2 + \ldots\;,$$

where $c_0, c_1, c_2, \ldots \in \{0,1,\ldots,p-1\}$, and write

$$\zeta_h = \zeta_h(\xi) = c_0 + c_1p + \ldots + c_{h-1}p^{h-1} \quad (h \geq 1). \tag{4.10}$$

Since $|\xi-\zeta_h|_p \leq p^{-h}$, we immediately obtain the following lemma.

Lemma 4.5. Let A, B be rational integers not both 0 and let h be any positive integer. Then $|B\xi - A|_p \leqslant p^{-h}$ if and only if $|B\zeta_h - A|_p \leqslant p^{-h}$, where ζ_h is as defined in (4.10).

We now proceed to construct a Mahler II continued fraction for ξ. For $h \geqslant 1$, put

$$\alpha(h) = \zeta_h/p^p ,$$

and so

$$0 \leqslant \alpha(h) < 1 .$$

Now construct the ordinary continued fraction for $\alpha(h)$, say

$$\alpha(h) = \frac{1}{a_1(h)+}\,\frac{1}{a_2(h)+}\,\cdots + \frac{1}{a_{N_h}(h)} .$$

Let $R_n(h)/B_n(h)$ for $n = -1, 0, 1, \ldots, N_h$ denote the n^{th} convergents of the continued fraction of $\alpha(h)$ with the convention that

$$R_{-1}(h) = 1,\ B_{-1}(h) = 0,\ R_0(h) = 0,\ B_0(h) = 1.$$

Evidently, we have

$$R_n(h) = a_n(h)R_{n-1}(h) + R_{n-2}(h) \qquad (n = 1, 2, \ldots, N_h),$$

$$B_n(h) = a_n(h)B_{n-1}(h) + B_{n-2}(h) .$$

Now define

$$A_n(h) = \zeta_h B_n(h) - p^h R_n(h) \qquad (n = -1, 0, 1, \ldots, N_h).$$

It is clear that for all n, the greatest common divisor of $A_n(h)$ and $B_n(h)$, $(A_n(h), B_n(h))$, is a divisor of p^h, and $R_n(h), B_n(h) > 0$ for all $n \geqslant 1$. In fact, Mahler [25] pages 64-67 shows that for some n we have

$$|A_n(h)| \leqslant p^{h/2}, \quad |B_n(h)| \leqslant p^{h/2} .$$

(We refer to Mahler [25] for the proof, which depends only on standard properties of the continued fraction of $\alpha(h)$ but is notationally complex.) Thus, by Lemma 4.5 the pair

$A = A_n(h)$, $B = B_n(h)$ satisfies (4.1) and we have the following theorem.

Theorem 4.6. Let $h \in Z^+$; ξ and ζ_h be as in (4.10). Then there exist non-zero integers A, B satisfying (4.1) and such that

$$A = \zeta_h B - p^h R,$$

where $R > 0$, $B > 0$ and R/B is one of the convergents of the ordinary continued fractions of ζ_h / p^h.

For each $n \in Z^+$, let (A_n, B_n) be a solution of (4.1) obtained by applying Theorem 4.6 with $h_1 \geq 1 + 2h(\xi)$ and $h_n = n$ (or $n + 2h(\xi)$). We now wish to construct a Mahler II continued fraction for ξ. There are two conditions that must be satisfied, they are

$$\Delta_n = A_{n-1}B_n - A_n B_{n-1} \neq 0 \qquad (n \geq 0)$$

$$\delta_n = A_{n-1}B_{n+1} - A_{n+1}B_{n-1}$$

(as usual, we set $A_{-1} = 1$, $B_{-1} = 0$, $A_0 = 0$, $B_0 = 1$); and as we have seen from results in Chapter 2, it is natural to require that

$$M_{n+1} = \max(|A_{n+1}|, |B_{n+1}|) > M_n = \max(|A_n|, |B_n|) \qquad (n \geq 0).$$

It is easily seen that we can satisfy these three requirements by extracting pairs of subsequences for which the value of M are strictly increasing and the value of $|\xi - A/B|_p$ are strictly decreasing. Let (A_n, B_n) be a pair of such subsequences obtained by omitting as few pairs (A_n, B_n) as possible. Then, by section 3 of Chapter 2, the sequences $(A_n), (B_n)$ determine a continued fraction converging to ξ and we call this a Mahler II continued fraction of ξ. It is clear from the construction that the convergents A_n/B_n of such a continued fraction satisfy

$$|\xi - A_n/B_n|_p \leqslant M_n^{-2} = \left(\max(|A_n|,|B_n|)\right)^{-2} .$$

However, they will not in general satisfy the other conditions in (4.5) and the above condition by itself is not quite enough to prove weak periodicity of the continued fraction of a quadratic irrational by Theorem 2.12.

5. Derivation of Mahler I from Mahler II.

For Mahler I, we considered solutions (A,B) of (4.1) for certain values of h $(h = h_n)$, and required in addition certain best approximation properties for these pairs (A,B). For Mahler II, we considered solutions of (4.1) for all $h \geqslant 2h(\xi) + 1$, but restricted our attention to those pairs constructed by the method of Theorem 4.6 and by certain restrictions described earlier. We now show how to obtain the pairs required for Mahler I by starting with the method of Theorem 4.6. This is equivalent to obtaining Mahler I convergents from Mahler II convergents.

For simplicity we suppose ξ is a p-adic unit, $|\xi|_p = 1$. We start with a lemma about the solutions of (4.1).

Lemma 4.7. Let $h \in Z^+$, ζ_h be as in (4.10) if $p \neq 2$, and further assume $h \geqslant 3$ if $p = 2$. Suppose that $(A,B) = (X,Y)$ and $(A,B) = (\mathcal{A},\mathcal{B})$ are two solutions of (4.1) such that

$$Y > 0, \quad \mathcal{B} > 0, \quad X/Y \neq \mathcal{A}/\mathcal{B} .$$

Let R be the positive integer such that

$$\mathcal{A} - \zeta_h \mathcal{B} = \pm p^h R .$$

Then

$$X = Y\zeta_h \pm p^h Z \tag{4.11}$$

where Y,Z are positive integers such that

(4.12) $$YR - Z\mathcal{B} = \pm 1$$

Proof. We first observe that since (X,Y) and $(\mathcal{A},\mathcal{B})$ satisfy (4.1) then neither of the four integers $X,Y,\mathcal{A},\mathcal{B}$ is zero and there is a positive integer Z such that (4.11) holds. Consider

$$|X\mathcal{B}-Y\mathcal{A}|_p = |(X-Y\xi)|\mathcal{B} - (\mathcal{A}-\mathcal{B}\xi)Y|_p \leqslant p^{-h},$$

then there are two cases to be examined.

Case 1: X and $\mathcal{A}$ both have the same sign. In this case, we get

$$|X\mathcal{B}-Y\mathcal{A}| < p^h ,$$

and so

$$|X\mathcal{B}-Y\mathcal{A}|_p|X\mathcal{B}-Y\mathcal{A}| < 1,$$

which yields $X\mathcal{B} - Y\mathcal{A} = 0$, contradicting the hypothesis that $X/Y \neq \mathcal{A}/\mathcal{B}$. Thus this case is not possible.

Case 2: X and $\mathcal{A}$ have different signs. We have then

$$|X\mathcal{B}-Y\mathcal{A}| \leqslant 2p^h.$$

If $|X\mathcal{B}-Y\mathcal{A}| = 2p^h$, then necessarily

$$|X| = |\mathcal{A}| = p^{\frac{1}{2}h} = Y = \mathcal{B}.$$

From $|Y\xi-X|_p \leqslant p^{-h}$ and $|\mathcal{B}\xi-\mathcal{A}|_p \leqslant p^{-h}$, we get

$$|\xi+1|_p \leqslant p^{-\frac{1}{2}h}, \quad |\xi-1|_p \leqslant p^{-\frac{1}{2}h}$$

which implies that $|2|_p \leqslant p^{-\frac{1}{2}h}$; this is absurd as either $p \neq 2$ or $h \geqslant 3$. Hence we must have $|X\mathcal{B}-Y\mathcal{A}| < 2p^h$, that is, p^h divides $X\mathcal{B} - Y\mathcal{A}$. Taking into account the fact that (4.1) is satisfied and the hypothesis $X/Y \neq \mathcal{A}/\mathcal{B}$, we arrive that the only possibilities are

$$X\mathcal{B} - Y\mathcal{A} = \pm p^h .$$

Substituting $\mathcal{A} = \pm p^h R + \zeta_h \mathcal{B}$ and using (4.11) in the above equation, we obtain (4.12).

We now combine the result with Theorem 4.6 to give our construction.

Construction: Suppose $h \geq 1$ and we wish to find a Mahler I approximation corresponding to this value of h, that is a solution (A,B) of (4.1) for which (A,B) is a power of p (by (4.5)) and $E(A,B)$ is minimal.

First we apply Theorem 4.5 to obtain a solution $(A,B) = (\mathcal{A},\mathcal{B})$, say, such that

$$\mathcal{A} = \zeta_h \mathcal{B} - p^h R ,$$

$R > 0$, $\mathcal{B} > 0$ and $R/\mathcal{B}$ is one of the ordinary convergents of ζ_h/p^h. Since ξ is a unit, ζ_h/p^h is not an integer, and so there is another convergent, already calculated, which immediately precedes or follows $R/\mathcal{B}$. Let this be z/y. Then

$$yR - z\mathcal{B} = \varepsilon, \quad -yR + z\mathcal{B} = -\varepsilon ,$$

where $\varepsilon \in \{-1,1\}$. Then any solution (Y,Z) of (4.12) is of the form

$$(Y,Z) = \pm (y,z) + t(\mathcal{B},R) \qquad (t \in \mathbb{Z}).$$

We look at the pairs (Y,Z) as above for which $0 < Y \leq p^{h/2}$ and

$$|Y\zeta_h \pm p^h Z| \leq p^{h/2} .$$

For any such pair, the corresponding pair (X,Y) with X defined by (4.11) yields a solution $(A,B) = (X,Y)$ of (4.1). Lemma 4.7 ensures that all solutions (X,Y) with $X/Y \neq \mathcal{A}/\mathcal{B}$, $Y > 0$ are obtained by this method. Any other solution with (X,Y) a power of p is of the form

$$(X,Y) = \pm p^r (A,B) ,$$

so that

$$E(X,Y) = E(A,B) \ .$$

Hence, in order to find a solution (A,B) for which (A,B) is minimal we need only to look at $E(A,B)$ for (A,B) and for the pairs (X,Y) obtained above.

Since the number of values of Y to be considered in the above procedure is at most $2p^{h/2}/B$, the method is quite efficient.

The following examples illustrate the above discussion as well as the fact that Mahler II approximations are not necessarily the same as those of Mahler I.

Example 4.5.1. In Q_{11}, $\sqrt{-2}$ exists and is an 11-adic unit,

$$\sqrt{-2} = 3 + 9.11 + 4.11^2 + 1.11^3 + 4.11^4 + 4.11^5 + 1.11^6 + 5.11^7 + \ldots \ .$$

Two possible Mahler I continued fractions for $\sqrt{-2}$ are

(i) $$\sqrt{-2} = \frac{3}{1+}\ \frac{11/3}{7/3+}\ \frac{-11}{6+}\ \frac{-11}{6+}\ \frac{-11}{6+}\ \ldots$$

(ii) $$\sqrt{-2} = \frac{-2}{3+}\ \frac{33/2}{-7/2+}\ \frac{11/3}{7/3+}\ \frac{-11}{6+}\ \frac{-11}{6+}\ \ldots \ .$$

Using the same notation as above and consider the case $h = 1$.

Mahler I: $A = 3$, $B = 1$ or $A = -2$, $B = 3$

Mahler II: $\zeta_1 = 3$,

$$\alpha(1) = \frac{\zeta_1}{11} = \frac{3}{11} = \frac{1}{3+}\ \frac{1}{1+}\ \frac{1}{2} \ .$$

Computing all convergents, the only possible ones are

$$R(1) = 0,\ B(1) = 1,\ A(1) = 3.1 - 11.0 = 3,$$

and

$$R(1) = 1,\ B(1) = 3,\ A(1) = 3.3 - 11.1 = -2.$$

In this case all approximations of Mahler I can be directly got from Mahler II.

Example 4.5.2. In Q_{13}, $\sqrt{-1}$ exists and is a 13-adic unit,

$$\sqrt{-1} = 5 + 5.13 + 1.13^2 + 0.13^3 + 5.13^4 + 5.13^5 + 1.36^6 + \ldots .$$

Two possible Mahler I continued fractions for $\sqrt{-1}$ are

(i) $$\sqrt{-1} = \frac{-3}{2+}\ \frac{13}{-4+}\ \frac{26/3}{-5/3}\ \frac{13}{6+}\ \frac{39/2}{5/2+} \cdots$$

(ii) $$\sqrt{-1} = \frac{2}{3+}\ \frac{-13}{6+}\ \frac{13}{-6+}\ \frac{13}{6+}\ \frac{39/2}{5/2+} \cdots .$$

Consider the case $h = 1$.

Mahler I: $A = -3$, $B = 2$ or $A = 2$, $B = 3$.

Mahler II: $\zeta_1 = 5$,

$$\alpha(1) = \frac{5}{13} = \frac{1}{2+}\ \frac{1}{1+}\ \frac{1}{2} .$$

By checking all convergents, the only possible one is

$$R(1) = 1,\ B(1) = 2,\ A(1) = 5.2 - 13.1 = -3.$$

In this case Mahler II algorithm does not give the pair $A = 2$, $B = 3$. Now from the discussion above and from the convergents $0/1$, $1/3$ preceding and succeeding $\frac{1}{2}$ in the continued fraction of $\alpha(1) = 5/3$, we see that the pairs $(0,1)$ and $(1,3)$ satisfying

$$1 \cdot R - 0 \cdot B = 1 - 0 = 1,$$

$$3 \cdot R - 1 \cdot B = 3.1 - 1.2 = 1.$$

Thus any solution (Y,Z) of (4.12) are either of the form

$$(Y,Z) = \pm(1,0) + t(2,1) \qquad (t \in \mathbb{Z}).$$

Alternatively, any such pair is of the form

$$(Y,Z) = \pm(3,1) + t(2,1) \qquad (t \in \mathbb{Z}).$$

The only pair (Y,Z) such that $0 < Y \leqslant 13^{\frac{1}{2}}$ and

$$|Y \cdot 5 \pm 13 \cdot Z| \leqslant 13^{\frac{1}{2}}$$

is $(3,1)$ and hence the corresponding (X,Y) with X defined by (4.11) is $(X,Y) = (3 \cdot 5 - 13 \cdot 1, 3) = (2,3)$, which is the other approximation of Mahler I.

CHAPTER 5

COMPARISON, APPLICATION AND OTHER METHODS

1. Introduction.

In this chapter we review and compare the various p-adic continued fractions studied in Chapters 3 and 4, and consider their effectiveness as tools for proving results in p-adic diophantine approximation. In section 2, we shall summarise and compare the properties of the continued fractions of Ruban, Schneider and Mahler and in section 3, we shall give some applications of these continued fractions. Section 4 will be the comparison of the results of section 3 with those obtained by Lutz [19] by methods which do not involve an approximation algorithm. A brief description of the geometrical approximation algorithm of Mahler will be given in section 5 and then followed by the comparison of results obtained by this method with those of section 3. Finally, in section 6, we shall give some conclusions about the relative value of the various algorithms and methods as tools for diophantine approximation.

2. Comparison of the various p-adic continued fractions.

We first review the nature of the various continued fraction algorithms.

Let $\xi \in pZ_p \sim \{0\}$. The Ruban algorithm gives a simple explicit construction of a unique sequence (b_n) of rationals such that

$$\xi = \frac{1}{b_0+}\,\frac{1}{b_1+}\,\frac{1}{b_2+}\,\cdots\quad ,$$

where $b_n \in J$, as defined by (3.5), and of a corresponding pair of sequences $(\alpha_n),(\beta_n)$ of rational integers such that

(5.1) $$\xi = \frac{\alpha_0}{\beta_0+}\,\frac{\alpha_1}{\beta_1+}\,\frac{\alpha_2}{\beta_2+}\,\ldots\,,$$

where $\alpha_n = p^{r_n}$ $(r_n \in Z^+)$, $\beta_n \in Z^+$ and $|\beta_n|_p = 1$ for all n. The algorithm can be expressed in terms of a transformation T such that

$$b_n(\xi) = b_0(T^n\xi).$$

Similarly, the Schneider algorithm gives a simple explicit construction of two unique sequences $(a_n),(b_n)$ of rational integers such that

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\ldots\,,$$

where $a_n = p^{s_n}$ $(s_n \in Z^+)$, $b_n \in \{1,2,\ldots,p-1\}$ for all n, and this algorithm can also be expressed in terms of a transformation T. In both cases, the transformation T is ergodic and because of this, certain metrical properties can be proved. The set of all Ruban continued fractions is exactly specified by the sequences (b_n), where $b_n \in J$ for all n, and similarly for the set of all Schneider continued fractions.

The Mahler II algorithm gives a systematic way of constructing a (not necessarily unique) sequence of approximations (A_n/B_n) and hence two sequences of rational numbers (a_n), (b_n) such that

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\,\ldots\,.$$

Because of the non-uniqueness of approximations, there may be more than one Mahler II continued fraction for ξ. From the approximations calculated by the Mahler II algorithm, a sequence of <u>best</u> approximations (A_n/B_n) as required for a Mahler I continued fraction can be derived by the method discussed at the end of Chapter 4, and then two sequences $(a_n),(b_n)$ of rational numbers can be obtained such that ξ has a Mahler I continued fraction

$$\xi = \frac{a_0}{b_0+}\,\frac{a_1}{b_1+}\,\frac{a_2}{b_2+}\cdots,$$

which is again not unique. Partly because of their non-uniqueness, the Mahler continued fractions do not correspond to obvious ergodic transformations T; this suggests that metrical results as obtained in the cases of Ruban and Schneider continued fractions cannot be expected. Further, it is not easy to determine whether a given continued fraction is a Mahler I or Mahler II continued fraction.

We now compare the sizes of the error in the various continued fractions. In each case, we let $(A_n),(B_n)$ be the sequences defined by (2.2) for the given continued fraction, so that the n^{th} convergent is A_n/B_n and

$$M_n = \max(|A_n|,|B_n|).$$

For the Ruban continued fraction, we also consider the sequences $(\mathcal{A}_n),(\mathcal{B}_n)$ corresponding to (5.1) in a similar way. From Theorems 3.2 (ii), 3.3, 3.5, 3.17 (ii), 3.18 and (4.3), we get

Ruban: $\quad |\xi - A_n/B_n|_p = |B_nB_{n+1}|_p^{-1} = |b_0^2b_1^2\dots b_{n-1}^2b_n|_p^{-1}$,

$$\frac{1+\alpha_1^{-1}+\dots+\alpha_n^{-1}}{\mathcal{M}_n\mathcal{M}_{n+1}} < |\mathcal{B}_n\xi-\mathcal{A}_n|_p \leqslant \frac{2^{n-1}}{\mathcal{M}_n\alpha_n};$$

Schneider: $\quad \dfrac{1+a_1^{-1}+\dots+a_n^{-1}}{M_nM_{n+1}} \leqslant |B_n\xi-A_n|_p = (a_0a_1\dots a_n)^{-1}$

$$\leqslant \frac{1}{M_na_n};$$

Mahler I: $\quad \tfrac{1}{2}M_n^{-1}M_{n+1}^{-1} \leqslant |B_n\xi-A_n|_p \leqslant p^{\frac{1}{2}}M_n^{-1}M_{n+1}^{-1}$;

Mahler I and II: $\quad |\mathcal{B}_n\xi-A_n|_p < M_n^{-2}$.

From the above estimates, it is clear that the Mahler I algorithm is the best for approximation purposes.

The second comparison is finiteness. Trivially, for any one of the continued fractions if the continued fraction is finite, then it represents a rational number (Theorem 2.7). The converse result is true for Mahler I and II continued fractions by Theorem 2.13. However, as seen in sections 3.4 and 3.8, there are rational numbers having infinite Ruban and Schneider continued fractions and so the converse result is not generally true unless a stronger approximation property such as (ii) of Theorem 2.13 holds, that is

$$|B_n\xi - A_n|_p < cM_n^{-2} \qquad (n \geqslant 1),$$

where c is a constant independent of n.

The third comparison is periodicity. Theorem 2.8, that a periodic continued fraction represents a number that satisfies a quadratic equation with rational integral co-efficients, holds true for all continued fractions. The converse result holds in a weaker form for Mahler I continued fractions as seen in Theorem 4.7 that if $\xi \in p\mathbb{Z}_p \sim \{0\}$ is a quadratic irrational, then its Mahler I continued fraction is weakly periodic (as defined in section 4 of Chapter 2). For Ruban and Schneider continued fractions, the proof that works in the case of Mahler I does not apply, as mentioned at the end of sections 3 and 6 of Chapter 3. As for Mahler II continued fractions, it is not clear whether the condition (iii) of Lemma 2.11 holds, and so the proof of Theorem 2.12 does not apply.

3. Applications of p-adic continued fractions to diophantine approximations.

In Chapter 1 (section 3) we have seen that classical continued fractions can be applied to derive a number of diophantine approximation results. The p-adic analogues of some of these results will be discussed here. First of all, we re-state results already obtained which may be regarded as analogues of Dirichlet's thoerem and Hurwitz's theorem (Theorem 1.12).

Theorem 5.1A (p-adic Dirichlet-Hurwitz theorem).

(i) For any given positive integer h and any p-adic integer ξ, there are two rational integers A,B not both 0 such that

$$|A-B\xi|_p \leqslant p^{-h}, \quad \max |A|,|B|) \leqslant p^{\frac{1}{2}h} .$$

(ii) Let $\xi \in Z_p$ be irrational. Then there are infinitely many pairs of integers A,B such that

$$|A-B\xi|_p < \left(\max(|A|,|B|)\right)^{-2} .$$

Proof. (i) is Corollary 1.18 (also Lemma 4.1).

(ii) follows easily from this or is immediate using the Mahler I or II algorithm.

Now we look at analogues of Khintchine and Tchebycheff's theorems (which can be derived from each other as in the classical case).

Theorem 5.2A (p-adic Khintchine Theorem). Let $\xi \in Z_p \sim \{0\}$ be irrational. Then there exist arbitrarily large positive numbers $t \geqslant 1$ such that

$$\max(|A|,|B|)\,|A-B\xi|_p < 1/4\sqrt{p}\; t ,$$

$$1 \leqslant \max\,(|A|,|B|) \leqslant t ,$$

is not soluble in rational integers A,B.

Proof. Let $(A_n),(B_n)$ be two sequences of rational integers corresponding to a Mahler I continued fraction of ξ and such that A_n/B_n denotes the n^{th} convergent of this continued fraction. Take a large $n \in Z^+$ such that

$$M_{n+1} > 2\sqrt{p}\,\max(|A|,|B|)\ ,$$

where $M_{n+1} = \max(|A_{n+1}|,|B_{n+1}|)$. If

$$|A-B\xi|_p \leqslant |A_n-B_n\xi|_p\ ,$$

then by the construction of Mahler I continued fractions (Theorem 4.6),

$$\max(|A|,|B|) > M_n\ ,$$

and by the strong triangle inequality as well as the approximation property (4.6) of Mahler I, we get

$$\begin{aligned}|AB_n-A_nB|_p &= |B_n(A-B\xi)-B(A_n-B_n\xi)|_p\\ &\leqslant |A_n-B_n\xi|_p \leqslant \sqrt{p}\ M_n^{-1}M_{n+1}^{-1}\ .\end{aligned}$$

Also,

$$|AB_n-A_nB| \leqslant 2\ M_n\ \max(|A|,|B|)\ .$$

Thus

$$|AB_n-A_nB|\ |AB_n-A_nB|_p \leqslant 2\sqrt{p}\ M_{n+1}^{-1}\ \max(|A|,|B|) < 1.$$

Since $AB_n-A_nB \in Z$, it follows then that $AB_n-A_nB = 0$ and so there are non-zero integers f,g such that g is a power of p,

$$A = A_nf/g,\quad B = B_nf/g,\quad \left|\frac{f}{g}\right| > 1.$$

Therefore by the above estimates and the approximation property (4.6) of Mahler I, we obtain

$$\begin{aligned}\max(|A|,|B|)\ |A-B\xi|_p &= |f|\,|f|_p\ M_n|A_n-B_n\xi|_p\\ &\geqslant \tfrac{1}{2}M_{n+1}^{-1}\ .\end{aligned}$$

If $|A-B\xi|_p > |A_n-B_n\xi|_p$ and $AB_n - A_nB = 0$, then by the same kind of argument as in the previous case we obtain the same estimate

$$\max(|A|,|B|)|A-B\xi|_p > \tfrac{1}{2}M_{n+1}^{-1} \quad .$$

If $|A-B\xi|_p > |A_n-B_n\xi|_p$ and $AB_n - A_nB \neq 0$, then

$$\{2\max(|A|,|B|)\ M_n\}^{-1} \leqslant |AB_n-A_nB|^{-1} \leqslant |AB_n-AB_n|_p$$
$$= |B_n(A-B\xi)-B(A_n-B_n\xi)|_p \leqslant |A-B\xi|_p,$$

and so

$$\max(|A|,|B|)\ |A-B\xi|_p \geqslant \tfrac{1}{2}M_n^{-1} > \tfrac{1}{2}M_{n+1}^{-1} \quad .$$

Choosing $t = M_{n+1}/2\sqrt{p}$ in all cases, the theorem follows.

Theorem 5.2A was proved as above in Mahler [22] and was applied to prove the following theorem in the same paper.

Theorem 5.3A (p-adic Tchebycheff Theorem). Let ξ b e an irrational p-adic integer and ζ be any p-adic integer. Then there exists a positive number μ depending only on p but not on ξ and ζ such that the system of inequalities

$$|A-B\xi-\zeta|_p \leqslant \mu t^{-2} \ ,$$
$$\max\ (|A|,|B|) \leqslant t \ ,$$

is soluble in rational integers A,B for fixed arbitrarily large values of $t \geqslant 1$. ($\mu = ([p^2 4\sqrt{p}]!)^3/4\sqrt{p}$ is sufficient for this theorem.)

4. The method of Lutz.

In the monograph [19], E. Lutz studied the diophantine approximation problem of linear forms in many p-adic variables. The methods she uses come from the geometry of numbers and p-adic measure theory.

She first defines a hyperconvex form $f(x)$ as the mapping

$$f : \mathcal{Q}_p^n \to R$$

such that

(i) $f(x) \geqslant 0$ for all x in $\mathcal{Q}_p^n$

(ii) $f(tx) = |t|_p f(x)$ for all t in $\mathcal{Q}_p$

(iii) $f(x+y) \leqslant \max\big(f(x), f(y)\big)$ for all x, y in $\mathcal{Q}_p^n$.

To study the values taken by a hyperconvex form, it is shown to be sufficient to consider problems on linear forms with p-adic coefficients. She then defines the lattice defined by the inequality $f(x) \leqslant c$ where c is a positive constant as the set of points x in $\mathcal{Q}_p^n$ with rational integral coefficients; this set is a sublattice of Z^n in the classical sense of the geometry of numbers. A connection of this lattice with the measure of the set $\{x \in Z_p^n;\ f(x) \leqslant c\}$ is then established as well as a number of theorems on the existence of points $x \in Z^n$ satisfying $f(x) \leqslant c$ and other conditions involving a norm function g defined on R^n.

The applications of her method to diophantine approximations is made by putting

$$f(x) = \max_{1 \leqslant j \leqslant n} |p^{-\lambda_j} \Lambda_j(x)|_p, \quad g(x) = H(x) = \max_{1 \leqslant j \leqslant n} |x_j| ,$$

where $\Lambda_1, \ldots, \Lambda_n$ are linear forms in n variables with p-adic coefficients and $\lambda_1, \ldots, \lambda_n$ are rational integers. This f is shown to be hyperconvex and by applying previous results as well as introducing a number of definitions, results on diophantine approximation for a system of linear forms with p-adic coefficients are obtained, including, in particular, Theorem 5.1A. We present here a few special cases, corresponding to Lutz's Theorems 2.11 and 2.12, to compare with Theorems 5.2A and 5.3A.

Theorem 5.2B. Let ξ be an irrational p-adic unit. Then there are infinitely many rational integers n such that

$$|A+B\xi|_p \leqslant p^{-n}$$

has no solution $(A,B) \in Z^2$ such that

$$0 < \max(|A|,|B|) \leqslant p^{\frac{1}{2}n}/\sqrt{2}\ p^{\frac{1}{4}} \ .$$

Theorem 5.3B. Let ξ be an irrational p-adic unit. Then for any p-adic unit ζ, there are infinitely many n such that

$$|A+B\xi+\zeta|_p \leqslant p^{-n}$$

has a solution in Z^2 such that

$$\max\ (|A|,|B|) \leqslant \tfrac{1}{2}(1+\sqrt{2}p^{\frac{1}{4}})\ p^{\frac{1}{2}n} \ .$$

In the later part of the monograph, Lutz obtains multi-dimensional metrical results. The following theorem, which is a special subcase of the case $n = 2$, $p = 1$ of her Theorem 4.24, is a p-adic analogue of Theorem 1.15.

Theorem 5.4. Let $f(\ell)$ be a well-defined positive real-valued function of positive variable ℓ. Then the number of solutions $(A,B) \in Z^2$ of

$$|A+B\xi|_p \ \leqslant\ f(\max|A|,|B|)$$

is finite or infinite for almost all $\xi \in Z_p$ depending as to whether the series

$$\sum_{h=1}^{\infty} h\ f(h)$$

converges or diverges.

5. The geometrical algorithm of Mahler.

In the paper [23], K. Mahler employs a geometrical method based on modular transformations in the complex plane C to study the approximation properties of p-adic integers.

His algorithm will be briefly discussed in this section.

Let

$H = \{z = x+iy \in C;\ y \geqslant 0\}$, the upper half plane of C,

$F = \{z = x+iy \in H;\ -\frac{1}{2} \leqslant x < \frac{1}{2}, x^2+y^2 > 1\}$, the fundamental domain,

$\Gamma = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a,b,c,d \in Z \text{ and } |ad-bc| = 1\right\}$, the modular group of transformations,

λ be a fixed but arbitrary point in F, and ξ be a p-adic integer to be approximated.

For $n = 0,1,2,\ldots$, define integers C_n, c_n by

$$|\xi - C_n|_p \leqslant p^{-n}, \quad 0 \leqslant C_n \leqslant p^{n-1},$$

$$c_n = (C_{n+1} - C_n)/p^n,$$

so that

$$\xi = \lim_{n\to\infty} C_n = c_0 + c_1 p + c_2 p^2 + \ldots,$$

and that the sequence $C(\xi) = (C_n)$ as well as the sequence $c(\xi) = (c_n)$ uniquely determine ξ. Next, define the sequence $Z(\xi) = (z_n)$ in H by

$$Z_0 = \lambda, \quad Z_n = (C_n + \lambda)/p^n \qquad (n = 1,2,1,\ldots),$$

and then define the sequence $z(\xi) = (z_n)$ in F such that Z_n is equivalent to z_n for all n. (Two points in H are <u>equivalent</u> if they are related by an element of Γ). The sequence $z(\xi)$ is unique and is called the <u>representative</u> of ξ. The aim is to investigate $z(\xi)$ and its related modular transformations which will then lead to results on diophantine approximations of ξ.

Let the modular transformation connecting Z_n and z_n be

$$Z_n = \frac{R_n z_n + R_n'}{B_n z_n + B_n'}$$

with $|R_nB_n'-R_n'B_n| = 1$ and $(B_n, B_n') = 1$. Define the transformation

$$T_n = \begin{pmatrix} A_n & A_n' \\ B_n & B_n' \end{pmatrix} \qquad (n \geqslant 0)$$

where $A_n = p^n R_n - C_n B_n$, $A_n' = p^n R_n' - C_n B_n'$. Then $\det T_n = p^n$. Define

$$\Omega_{n+1} = T_n^{-1}\, T_{n+1} \qquad (n \geqslant 0),$$

and let $\Omega(\xi)$ denote the sequence (Ω_n). We have

$$\det \Omega_{n+1} = p, \quad T_n = \Omega_1\Omega_2\ldots\Omega_n \quad (n \geqslant 1).$$

It is shown that ξ determines $T(\xi)$, $\Omega(\xi)$ uniquely and conversely. By characterising the elements of $\Omega(\xi)$, three theorems stating the existence of ξ, corresponding to λ and $\Omega(\xi)$, that can be closely approximated by certain number z_n in F are obtained. It is now a matter of considering and characterising $z_n = x_n + iy_n$. The following are some interesting results proved.

(i) If $\xi \in Q$, then $\lim\limits_{n\to\infty} y_n = +\infty$.

(ii) If $\xi \in Z_p$ is irrational, then for infinitely many n,

$$y_n \leqslant \sqrt{p}\,,$$

and so

$$y(\xi) = \lim_{n\to\infty} \inf y_n \leqslant \sqrt{p}\,.$$

(iii) Given an $\varepsilon > 0$, there is an irrational p-adic integer ξ such that

$$y(\xi) \geqslant \sqrt{p} - \varepsilon\,.$$

Since the study of modular transformations is closely connected to the study of quadratic forms, it is natural to apply these results to diophantine approximation via quadratic forms. To this end, let

$$\varphi(X,Y) = \frac{2(X-\lambda Y)(X-\bar{\lambda}Y)}{|\lambda-\bar{\lambda}|} = \alpha X^2 + 2\beta XY + \gamma Y^2 ,$$

where $\bar{\lambda}$ denotes the complex conjugate of λ, be a positive definite quadratic form with determinant $\beta^2 - \alpha\gamma = -1$. This form φ is connected with T_n as defined earlier via λ and by considering

$$\varphi_n(X,Y) = \varphi(A_nX+A'_nY, B_nX+B'_nY) = \alpha_nX^2 + 2\beta_nXY + \gamma_nY^2 .$$

It is then seen that φ_n is related to z_n, defined above, by

$$\varphi_n(X,Y) = \alpha_n(X-z_nY)(X-\bar{z}_nY) ,$$

and also

$$\alpha_n = p^n/y_n = \varphi(A_n,B_n) ,$$

$$\beta_n = -p^nx_n/y_n = \alpha A_nA'_n + \beta(A_nB'_n+A'_nB_n) + \gamma B_nB'_n ,$$

$$\gamma_n = p^n(x_n^2+y_n^2)/y_n = \varphi(A'_n,B'_n) .$$

Using all these connections, a number of diophantine approximation results for ξ are obtained.

A sharper version of Theorem 5.1A is obtained for all p, and best possible versions of this corresponding closely to Hurwitz's classical results (Theorem 1.12) are obtained for $p = 2,3,5$. For example, his Theorem 19 gives the following result.

Theorem 5.1C For every 2-adic integer ξ and for at least one of any three consecutive integers n there are two integers A_n, B_n satisfying

$$|A_n+B_n\xi|_p \leqslant 2^{-n}, \quad 0 < \varphi(A_n,B_n) \leqslant \frac{2}{\sqrt{7}} \cdot 2^n ;$$

moreover the constant $2/\sqrt{7}$ is best possible.

The following, corresponding to his Theorems 23 and 26, are his analogues of Khintchine's and Tchebycheff's theorems.

Theorem 5.2C. (i) To every irrational p-adic integer ξ, there is an infinity of indices n for which the conditions

$$|A+B\xi|_p \leq p^{-n}, \quad 0 < \varphi(A,B) < p^n/\sqrt{p}$$

have no solution in rational integers A, B.

(ii) To every $\varepsilon > 0$, there is an irrational p-adic integer ξ such that for all sufficiently large n, there are two rational integers A_n, B_n satisfying

$$|A_n+B_n\xi|_p \leq p^{-n}, \quad 0 < \varphi(A_n,B_n) \leq \left(\frac{1}{\sqrt{p}} + \varepsilon\right) p^n,$$

while for an infinity of indices,

$$|A_n+B_n\xi|_p = p^{-n}, \quad p^n/\sqrt{p} \leq \varphi(A_n,B_n) \leq \left(\frac{1}{\sqrt{p}} + \varepsilon\right) p^n .$$

Theorem 5.3C. Let $\xi \in Z_p$ be irrational and let $\zeta \in Z_p$. Then there is an infinity of indices n, such that there are two rational integers A_n, B_n satisfying

$$|A_n+B_n\xi+\zeta|_p \leq p^{-n}, \quad \varphi(A_n,B_n) \leq p^n(p+1)/4\sqrt{p} .$$

Taking, for example $\varphi(A,B) = 2(A^2+AB+B^2)/\sqrt{3}$ in Theorem 5.2C, we see that this gives the bound $0 < \max(|A|,|B|) < 3^{\frac{1}{4}} (p^n/2p^{\frac{1}{2}})^{\frac{1}{2}}$, while Theorem 3.2B gives $0 < \max(|A|,|B|) < 1\cdot(p^n/2p^{\frac{1}{2}})^{\frac{1}{2}}$, which is only slightly better; yet because there are different choices for φ, we may say that in this case Lutz's and Mahler's geometrical methods are compatible. Moreover, both Theorems 5.2B and 5.2C are clearly sharper than Theorem 5.2A. By taking $\varphi(A,B) = A^2 + B^2$, it is easily seen that Theorem 5.3C implies Theorem 5.3B and Theorem 5.3B is clearly sharper than Theorem 5.3A. Hence Mahler's geometrical method is better than Lutz's method and than Mahler I.

6. Conclusion.

From the above comparison, it is clear that for approximation purposes, Mahler's geometrical method yields the best results, then come Lutz's method, Mahler I and Mahler II, while Ruban and Schneider algorithms are not as good. However both Mahler's geometrical and Lutz's method are not constructive while Mahler I, II, Ruban and Schneider algorithms are.

PART 2

INTERPOLATION

CHAPTER 6
INTRODUCTION AND PRELIMINARIES

In this chapter some background to p-adic interpolation will be given. In sections 1 and 2, certain basic ideas of classical approximation and interpolation will be recalled and a few examples of number theoretic applications of interpolation will be recollected. Section 3 will give a discussion of some previous work on p-adic approximation and interpolation. The scope of the work in the next two chapters will also be indicated. In the last section, a number of relevant ideas and preliminary results on p-adic analysis that will be used in Chapter 7 will be gathered together.

1. Classical approximation and interpolation.

The classical theory of approximation, as described, for example, in Cheney [10], mainly concerns the problem of approximating a given function f

$$f : [0,1] \to \mathbb{R},$$

say, by simpler functions such as polynomials. One of the most important theorems is the Weierstrass approximation theorem which states that for f as above and for each fixed $\varepsilon > 0$ there exists a polynomial $P(x)$ such that for all $x \in [0,1]$,

$$|f(x) - P(x)| < \varepsilon.$$

This theorem can be proved by various methods, for example by using the Bernstein polynomials

$$B_n(x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k} \qquad (x \in [0,1]). \tag{6.1}$$

Another alternative is by constructing a polynomial taking the same values as f at the zeros of the Tchebycheff polynomials

$$T_n(x) = \cos(n \cos^{-1}x) \qquad (x \in [0,1]). \tag{6.2}$$

Since the Tchebycheff polynomials are characterised by the fact that for each n, $T_n(x)$ $(x \in [0,1])$ deviates least from zero compared with any other polynomials of the same degree, then it is also clear that by using Tchebycheff polynomials we can obtain polynomials which best approximates f. A great deal more can also be said via the functional analytic approach.

The classical problem of interpolation as seen in Gelfond [14] is to determine a polynomial P_n of degree at most n such that

$$P_n(x_i) = f(x_i) \qquad (i = 0,1,\ldots,n)$$

where $x_0,\ldots,x_n$ are given distinct points and f is a given function. There is a convenient way of finding P_n using the idea of divided differences $[x_0,\ldots,x_i]$ defined by

$$(6.3) \qquad \begin{aligned} [x_0,x_1] &= \frac{f(x_0) - f(x_1)}{x_0 - x_1}, \\ [x_0,x_1,x_2] &= \frac{[x_0,x_1] - [x_1,x_2]}{x_0 - x_2}, \end{aligned}$$

and so on. It can be shown that the polynomial P_n exists, is unique and is given by

(i) <u>Lagrange's formula</u>

$$P_n(x) = \sum_{i=0}^{n} \frac{f(x_i)\varphi(x)}{(x-x_i)\varphi'(x_i)}, \tag{6.4}$$

where $\varphi(x) = (x-x_0)(x-x_1)\ldots(x-x_n)$, and also by

(ii) Newton's formula

$$(6.5)\qquad P_n(x) = \sum_{i=0}^{n} [x_0, x_1, \ldots, x_i](x-x_0)(x-x_1)\ldots(x-x_{i-1}),$$

and also, if f is analytic, by

(iii) Hermite's formula for complex-valued function f

$$(6.6)\qquad P_n(x) = \frac{1}{2\pi i}\int_c \frac{\varphi(u) - \varphi(x)}{\varphi(u)\ (u-x)} f(u)du,$$

where c denotes a suitable contour enclosing $x_0, \ldots, x_n$.

The corresponding error estimate for the first two forms is

$$(6.7)\qquad |R_n(x)| = |f(x)-P_n(x)| = |[x, x_0, x_1, \ldots, x_n]\varphi(x)|,$$

and for the third form is

$$(6.8)\qquad |R_n(x)| = |f(x)-P_n(x)| = \left|\frac{1}{2\pi i}\int_c \frac{\varphi(x) f(u)du}{\varphi(u)(u-x)}\right| .$$

Under suitable conditions the error gets smaller as n increases and then P_n is a good approximation to f. For a given sequence (x_n) of distinct points, we can find a sequence of polynomials (P_n) interpolating f at such points and if

$$P_n \to f \qquad \text{uniformly in } [0,1], \text{ say,}$$

then f is represented by the interpolation series

$$f(x) = \sum_{i=0}^{\infty} [x_0, x_1, \ldots, x_i](x-x_0)\ldots(x-x_{i-1}) \qquad (x \in [0,1]).$$

2. Number theoretic applications of interpolation.

The technique of interpolation has been applied to number theoretic problems, particularly in the theory of transcendence. The following are some examples. Let $a(k,\ell)$ $(1 \leq \ell \leq L;\ 0 \leq k \leq K-1)$, $\omega_1, \ldots, \omega_L$ be complex numbers with $\Delta = \max_{1 \leqslant i \leqslant L} |\omega_i|$. Define the exponential polynomial E by

$$E(z) = \sum_{k=0}^{K-1} \sum_{\ell=1}^{L} a(k,\ell)\ z^k e^{\omega_\ell z}.$$

The following theorem, which deals with some estimates concerning E which are of interest in transcendental number theory, can be proved by using interpolation.

Theorem 6.1. Let E, Δ be defined as above. Suppose that E is not identically zero. Then for some real $R > 0$, we have

(i) $$\max_{|z| \leqslant \gamma R} |E(z)| \leqslant \frac{\gamma^{KL}-1}{\gamma-1}\, e^{R\Delta(\gamma+1)} \max_{|z| \leqslant R} |E(z)| ,$$

for some real $\gamma > 1$,

(ii) the number of zeros of E in any closed disc, with radius R, counted with multiplicities is

$$h \ll KL + R\Delta ,$$

where $\ll$ signifies the inequality $\leqslant$ up to a constant.

Proof. Result (i) is Theorem 2 in Balkema and Tijdeman [7 ; page 122] and is also implicit in Baker [6 ; pages 120-122]. Result (ii) is Lemma 1, page 120 of Baker [6].

The almost-best known bound for h in (ii) above was obtained by Tijdeman as remarked by Baker [6 ; page 120]. It is

$$h \leqslant 3KL + 4R\Delta.$$

As well as proving (i) above, Balkema and Tijdeman in [7] also employ interpolation methods to prove the following versions of Turan's theorems, which have important applications in analytic number theory and diophantine approximation, as can be seen, for example, in Turan [41].

<u>Theorem 6.2</u>. (Turan's first main theorem.) Let m and n be non-negative integers, $n \geqslant 1$. Let $b_1,\ldots,b_n$ and $\alpha_1,\ldots,\alpha_n$ be sequences of complex numbers. Then there exists an integer ν with $m+1 \leqslant \nu \leqslant m+n$ such that

$$\left|\sum_{k=1}^{n} b_k \alpha_k^{\nu}\right| \geqslant \left(\sum_{h=1}^{n} \binom{m+h-1}{h-1} 2^{h-1}\right)^{-1} \left|\sum_{k=1}^{n} b_k\right| \min_{j=1,\ldots,n} |\alpha_j|^{\nu}.$$

<u>Theorem 6.3</u>. (Turan's second main theorem.) Let m and n be integers, $m \geqslant 0$, $n \geqslant 2$. Let $b_1,\ldots,b_n$ and $\alpha_1,\ldots,\alpha_n$ be sequences of complex numbers such that

$$0 = |\alpha_1 - 1| \leqslant |\alpha_2 - 1| \leqslant \ldots \leqslant |\alpha_n - 1|.$$

Then

$$\max_{\nu=m+1,\ldots,m+n} \left|\sum_{k=1}^{n} b_k \alpha_k^{\nu}\right| \geqslant \left(\frac{n-1}{4e(2m+3n)}\right)^{n-1} \min_{\ell=1,\ldots,n} \left|\sum_{k=1}^{\ell} b_k\right| .$$

If moreover $|\alpha_k| \leqslant 1$ for $k = 1,\ldots,n$, then

$$\max_{\nu=m+1,\ldots,m+n} \left|\sum_{k=1}^{n} b_k \alpha_k^{\nu}\right| \geqslant \left(\frac{n-1}{8e(m+n)}\right)^{n-1} \min_{\ell=1,\ldots,n} \left|\sum_{k=1}^{\ell} b_k\right| .$$

Further applications of classical interpolation are to be found in Gelfond [14], [15]. From these examples, it is evident that interpolation techniques should be useful in dealing with the corresponding number theoretic problems in p-adic fields.

3. <u>Approximation and interpolation for p-adic functions</u>.

The earliest work on p-adic approximation stemmed from a paper of Dieudonné [12] in 1944. Dieudonné was mainly concerned with approximation of continuous functions defined over a compact subset of $\mathcal{Q}_p$. Among various results, Dieudonné proved the following p-adic analogue of the Weierstrass approximation theorem:

Theorem 6.4. Let K be a compact subset of Q_p and f be a continuous function defined over K. To each $\varepsilon > 0$, there exists a polynomial g defined over Q_p such that for all $x \in K$, we have

$$|f(x) - g(x)|_p \leq \varepsilon.$$

Proof. See Theorem 4 page 86 of Dieudonné [12].

The problem of approximation to p-adic functions can also be regarded as a special case of approximation in the context of non-archimedean functional analysis. This area of research was started in 1943 by A.F. Monna (see his book [29] for a survey of the work up to 1970). Monna [28] also started the investigation of best approximation in non-archimedean vector spaces in 1956. For remarks on this problem see Monna [28] and the book by Narici, Beckenstein and Bachman [30]. While many results suggest similarity to the classical case, there are also difficulties, for instance, it is clear that the Bernstein polynomials (6.1) do not necessarily converge to f and there does not seem to be a p-adic analogue to the Tchebycheff polynomials because there are infinitely many polynomials yielding best approximations to a given function.

The earliest work in p-adic interpolation was done by Mahler [24] in 1958. He considered interpolation at the points $0,1,2,\ldots$ of a function

$$f : Z_p \to Z_p ,$$

which can be shown to have a representation

$$(6.9) \qquad \sum_n a_n\binom{x}{n} = \sum_n \frac{a_n}{n!} x(x-1)\ldots(x-n+1)$$

$$= \sum_n [0,1,\ldots,n;f]x(x-1)\ldots(x-n+1),$$

where, by (6.3),

$$(6.10) \qquad a_n = n![0,1,\ldots,n;f] = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k),$$

For more details of Mahler's work see his book [26] and two closely related papers by Ahlswede and Bojanic [3] and Márki and Szabados [27]. Mahler's work deals with the connection between the sequence (a_n) and the analytic nature of f. For example, if a_n as given by (6.10) tends to zero, then the series (6.9) converges to f and f is continuous on Z_p and, conversely, if f is continuous then a_n tends to zero and (6.10) holds.

Amice [4] has further generalised some of Mahler's results to larger fields, and has based her work on non-archimedean functional analysis. For example, she proved the following.

Theorem 6.5. Let K be a local field with valuation $|\ |$. Let (q_n) be a sequence of distinct elements of K such that for $|x| \leqslant 1$,

$$\prod_{i=0}^{n-1} \left|\frac{x-q_i}{q_n-q_i}\right| \leqslant 1 .$$

Let f be continuous on $|x| \leqslant 1$. Then

$$f(x) = \sum_{n=0}^{\infty} [x_0,\ldots,x_n;f] \prod_{i=0}^{n-1} \left(\frac{x-q_i}{q_n-q_i}\right) .$$

Just as in the classical situation it is helpful to work in the complex field C and use complex function theory, so in the p-adic case it is helpful to work in the field Ω_p, that is, the completion of the algebraic closure of Q_p. Working in this field Adams [1] employed the Schnirelman integral to prove p-adic transcendence results. There is a close connection between p-adic interpolation and the Schnirelman integral via formulae corresponding to (6.6) and (6.8). Indeed, Shorey [38], [39] used the interpolation method with Schnirelman integrals to prove p-adic transcendence results corresponding to those in Theorem 6.1. Recently van der Poorten [33], using the p-adic interpolation alone, was able to improve on Shorey's results. In particular he proved

Theorem 6.6. Let $\theta > 0$ be fixed. Let $E(z)$ be a p-adic exponential polynomial of the shape

$$E(z) = \sum_{k=1}^{m} \sum_{s=1}^{\rho(k)} a_{ks} z^{s-1} e^{\omega_k z} \qquad (a_{ks} \in \Omega_p, \omega_k \in \Omega_p)$$

with distinct ω_k such that $|\omega_k|_p \leqslant p^{-\left(\frac{1}{p-1}+\theta\right)}$, and let $n = \sum_{k=1}^{m} \rho(k)$. Then either the number of zeros of $E(z)$ in $|z|_p \leqslant 1$ is less than

$$(n-1) + \max_{0 \leqslant r < p-1} \{[\log_p(n+r)] - r/(p-1)\}/\theta$$

(where the square bracket denotes the integral part) or E vanishes identically.

This theorem was derived by van der Poorten from the following result on bounds for the coefficients of exponential polynomials, which was also proved in [33].

Theorem 6.7. Let E, n be as in Theorem 6.6. For each k $(k=1,\ldots,m)$, let δ_k be such that

$$|\omega_k - \omega_h|_p \geqslant p^{-\delta_k} \qquad (h \neq k;\ h = 1,\ldots,m)$$

Also let $\beta_1,\ldots,\beta_m$ be distinct points of Ω_p satisfying

$$|\beta_h|_p \leqslant 1 , \qquad |\overset{\beta}{\cancel{\alpha}}_h - \overset{\beta}{\cancel{\alpha}}_k|_p \geqslant p^{-\varepsilon} \qquad (h \neq k;\ h,k=1,\ldots,m),$$

for some fixed $\varepsilon > 0$. Further let $r_1, \ldots, r_\ell$ be non-negative integers with the sum

$$r = \sum_{i=1}^{\ell} r_i \, .$$

If

$$r \geqslant (n-1) + [\log_p(n+p-1)]/\theta$$

and

$$|E^{(i)}(\beta_h)|_p \leqslant p^{-\chi} \qquad (1 \leqslant h \leqslant n;\ 1 \leqslant i \leqslant r_h),$$

for some real χ, then

$$|a_{ks}|_p < p^A \qquad \big(1 \leqslant k \leqslant m;\ 1 \leqslant s \leqslant \rho(k)\big),$$

where

$$\begin{aligned} A &= A(\chi, r, \varepsilon, n, s, \delta_k) \\ &= \chi - (r-1)\varepsilon - (n-s)\delta_k + \log_p \big(|(s-1)!|_p\big) \\ &\quad - [\log_p(n+p-1)] + (n-1)/(p-1) \\ &\quad + \min\{(i-1)\varepsilon + \log_p\big(|(i-1)!|_p\big)\} \end{aligned}$$

where the minimum in the last term is over all $1 \leqslant i \leqslant r_h$, $1 \leqslant h \leqslant n$.

In Chapter 7, I shall develop p-adic interpolation technique using Schnirelman integrals and divided differences with an emphasis on analytic functions in Ω_p, and then I shall derive some number theoretic applications in Chapter 8.

4. Preliminaries on p-adic analysis.

We collect together here (mostly without proof) those results on p-adic function theory which will be used later and the proofs of which can be found in Adams [1], Adams and Straus [2] and Bachman [5].

From now on the work will be done in Ω_p unless indicated otherwise, and we consider p-adic functions

$$f : A \to B$$

where $A, B \subset \Omega_p$.

Definition 6.8. The first derivative f' of f is defined by

$$f'(w) = \lim_{z \to w} \frac{f(z) - f(w)}{z - w}$$

provided this limit exists. The following notation is also used

$$f'(w) = [Df(z)]_{z=w} = [D_z f(z)]_{z=w}$$

and successively, we define

$$f^{(0)} = f, D^{n+1}f = f^{(n+1)} = (f^{(n)})' \qquad (n \in Z^+) .$$

From now on, all limits considered are defined with respect to the p-adic valuation. We also note that with the above definition, the manipulation of p-adic differentiation corresponds exactly to that in the real case. (It is worth remarking that one major difference is that there exist many non-constant functions f with Df identically zero).

Definition 6.9. For some fixed a in Ω_p, f is said to be analytic in $|Z-a|_p \leq R$, where $R > 0$, if and only if it is representable as a power series in this disc

$$f(z) = \sum_{r=0}^{\infty} A_r (z-a)^r \qquad (|z-a|_p \leq R),$$

where $A_0, A_1, A_2, \ldots \in \Omega_p$. ($f$ is said to be analytic in $|z-a|_p < R$ if it is representable by a power series in $|z-a|_p < R$.)

We note that, since Ω_p is a non-archimedean field, each of the discs $|z-a|_p \leq R$ and $|z-a|_p < R$ is both open and closed. Moreover, since Ω_p is not a local field and hence not locally compact (see, for example, Theorem 1 page 23 and Corollary page 25 of Narici, Beckenstein and Bachman [30]), neither of these discs can be compact. If a power series representation of f exists in $|z-a|_p \leqslant R$, then it is unique, and since $A_n R^n \to 0$ $(n \to \infty)$, the convergence is uniform on $|z-a|_p \leqslant R$. The classical properties of power series apply without change. In particular, for f as above it is easily seen that f is differentiable arbitrarily often on $|z-a|_p \leqslant R$ (provided limits are interpreted relative to this set) and

$$f^{(r)}(z) = \sum_{n=r}^{\infty} A_n n(n-1)\ldots(n-r+1)(z-a)^{n-r} \qquad (|z-a|_p \leqslant R).$$

Also, it is easily shown that if f as above is not identically zero, then its zeros in $|z-a|_p \leqslant R$ are isolated; the number of such zeros is then also finite, as we shall show later (Corollary to Theorem 7.8).

<u>Definition 6.10</u>. For fixed $a, r \in \Omega_p$ the <u>Schnirelman integral</u> of f at the centre a with radius r, if it exists, is defined as

$$\int_{a,r} f = \int_{a,r} f(z)\,dz = \lim_{\substack{n\to\infty \\ |n|_p=1}} \sum_{k=1}^{n} f\big(a+r\xi_k(n)\big),$$

where $\xi_k(n)$ $(k=1,\ldots,n)$ denote all nth roots of unity in Ω_p.

<u>Proposition 6.11</u>. Let f, a, r be as in Definition 6.10. If $\int_{a,r} f(z)\,dz$ exists, then

$$\left|\int_{a,r} f(z)\,dz\right|_p \leqslant \max_{|z|_p=|r|_p} |f(a+z)|_p\ .$$

(For proof, see Adams [1 ; Theorem 1 page 298].)

Proposition 6.12. Let a, r be as in Definition 6.10. Let

$$f(z) = \sum_{t=0}^{\infty} a_t f_t(z)$$

where the series on the right converges uniformly to f on $|z-a|_p = |r|_p$. Suppose that for all t, $\int_{a,r} f_t$ exists. Then $\int_{a,r} f$ exists and

$$\int_{a,r} f = \sum_{t=0}^{\infty} a_t \int_{a,r} f_t .$$

(For proof, see Adams [1 ; Theorem 2 page 298].)

Proposition 6.13 (p-adic analogue of Cauchy integral theorem). Let $R > 0$ be real; $w, a, r \in \Omega_p$ be such that $|w|_p$, $|a|_p$, $|r|_p$ all $\leqslant R$. If f is analytic in $|z|_p \leqslant R$ and $|w-a|_p < |r|_p$, then

$$f^{(n)}(w) = n! \int_{a,r} \frac{f(z)(z-a)dz}{(z-w)^{n+1}} \qquad (n = 0, 1, 2, \ldots).$$

(See Theorem 7 page 300 of Adams [1].)

Proposition 6.14 (p-adic maximum modulus theorem). Let f be analytic in $|z|_p \leqslant R$ $(R > 0)$ and let

$$M(\alpha) = \max_{|z|_p = \alpha} |f(z)|_p .$$

Then

(i) $$M(\alpha) = \max_{n \geqslant 0} |a_n|_p \, \alpha^n ,$$

(ii) for $\alpha_1 \leqslant \alpha_2 \leqslant R$, we have

$$M(\alpha_1) \leqslant M(\alpha_2) \leqslant M(R) .$$

(See Lemma of Adams and Straus [2] and Theorem 9 page 301 of Adams [1].)

<u>Proposition 6.15</u> (p-adic Cauchy's inequality). Let f be analytic in $|z|_p \leqslant R$ $(R > 0)$. For any fixed $r \in \Omega_p$ such that $|r|_p \leqslant R$, we have

$$\left|\frac{f^{(n)}(z)}{n!}\right|_p \leqslant |r|_p^{-n} \max_{|z|_p=|r|_p} |f(z)|_p \qquad (|z|_p < |r|_p).$$

(See Theorem 9 page 301 of Adams [1].).

<u>Proposition 6.16</u> (p-adic residue theorem). Let f be analytic in $|z|_p \leqslant R$ $(R > 0)$. Let $r \in \Omega_p$ be such that $|r|_p \leqslant R$. Let also $k_1, \ldots, k_n$ be positive integers and

$$G(z) = (z-a_1)^{k_1}(z-a_2)^{k_2}\ldots(z-a_n)^{k_n}$$

be a polynomial with $|a_i|_p < |r|_p$ $(i = 1,\ldots,n)$. If $t \in \Omega_p \sim \{0\}$ is such that

$$|a_i - a_j|_p > |t|_p \qquad (i \neq j),$$

then

$$\int_{0,r} \frac{f(z)zdz}{G(z)} = \int_{a_1,t} \frac{f(z)(z-a_1)dz}{G(z)} + \ldots + \int_{a_n,t} \frac{f(z)(z-a_n)}{G(z)}dz$$

$$= \text{ sum of the residues of } f/G \text{ over all}$$

poles z such that $|z|_p < |r|_p$.

(See Theorem 13 and its corollary pages 302-304 of Adams [1].)

The residues are calculated as in the complex case. For example, if for some positive integer r

$$\psi(z) = g(z)/(z-b)^r, \quad |z-a|_p \leqslant |\rho|_p,$$

where g is analytic in $|z-a|_p \leqslant |\rho|_p$ and $|b-a|_p < |\rho|_p$, then the residue of ψ at b is

$$\operatorname{res}(\psi;b) = \frac{1}{r!}[D^{r-1}g(z)]_{z=b}.$$

Proposition 6.17 (p-adic Taylor's theorem). Suppose $f(z) = \sum_{n=0}^{\infty} A_n(z-a)^n$ is analytic in $|z-a|_p \leq R$ $(R > 0)$. Let $b \in \Omega_p$ be such that

$$|b-a|_p < R.$$

Then we can expand $f(z)$ about b,

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(b)}{n!} (z-b)^n \qquad (|z-b|_p < R).$$

(See Theorem 15 page 304 of Adams [1].)

Definition 6.18. The exponential function is defined as

$$\exp z = e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots$$

whenever the series converges.

Proposition 6.19. $\exp z$ is defined and analytic in $|z|_p < p^{-\frac{1}{p-1}}$ and $|\exp z|_p = 1$ and $|\exp(z) - 1|_p = |z|_p$ for all z in $|z|_p < p^{-\frac{1}{p-1}}$. (See Bachman [5] or Adams [1 ; page 306].)

Proposition 6.20. Let n be a non-negative integer. Write

$$n = a_0 + a_1 p + \ldots + a_t p^t ,$$

where t is a non-negative integer, $a_0, a_1, \ldots \in \{0,1,\ldots,p-1\}$ and $a_t \neq 0$. Then

$$|n!|_p = p^{-\frac{n-s}{p-1}} .$$

where $s = a_0 + \ldots + a_t$.

(See Bachman [5].)

We shall also need the following result on sequences of analytic functions, for which we outline the proof for the sake of completeness.

Proposition 6.21. Suppose that (f_n) is a sequence of functions which are analytic on $|z-a|_p \leqslant R$ and converge uniformly on $|z-a|_p \leqslant R$ to the function f. Then f is analytic on $|z-a|_p < R$.

Proof. Let $\rho \in \Omega_p$ be such that

$$|\rho|_p \leqslant R.$$

Since f_n is analytic in $|z-a|_p < |\rho|_p$, then

$$f_n(z) = \int_{a,\rho} \frac{f_n(u)(u-a)du}{u-z} \qquad (|z-a|_p < |\rho|_p).$$

Now

$$f(z) = \sum_{n=1}^{\infty} f_n(z) = \sum_{n=1}^{\infty} \int_{a,\rho} \frac{f_n(u)(u-a)du}{u-z}$$

and since $\sum f_n$ converges uniformly, by Proposition 6.12, we can interchange the summation sign with the integral sign and get

$$f(z) = \int_{a,\rho} \frac{f(u)(u-a)du}{u-z} \qquad (|z-a|_p < |\rho|_p)$$

Now consider for $|z-a|_p < |\rho|_p$ and large positive integer k,

$$F_k(z) = \sum_{n=1}^{k} f_n(z).$$

We have

$$F_k'(z) = \sum_{n=1}^{k} f_n'(z) = \sum_{n=1}^{k} \int_{a,\rho} \frac{f_n(u)(u-a)du}{(u-z)^2}.$$

Using the uniform convergence of $\sum f_n$, it is easily shown that uniformly

$$F_k'(z) \to f'(z) = \int_{a,\rho} \frac{f(u)(u-a)du}{(u-z)^2} \qquad (k \to \infty).$$

Similarly, we obtain

$$f^{(n)}(z) = n! \int_{a,\rho} \frac{f(u)(u-a)du}{(u-z)^{n+1}} \qquad (|z-a|_p < |\rho|_p)$$

Now for $|z-a|_p < |\rho|_p = |u-a|_p$, we have uniformly

$$\frac{u-a}{u-z} = 1 + \frac{z-a}{u-a} + \left(\frac{z-a}{u-a}\right)^2 + \ldots$$

Hence

$$f(z) = \int_{a,\rho} \frac{f(u)(u-a)dz}{u - z} = \int_{a,\rho} \left(\sum_{n=0}^{\infty} f(u)\left(\frac{z-a}{u-a}\right)^n\right)du$$

$$= \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} (z-a)^n \qquad (|z-a|_p < |\rho|_p)$$

and f is analytic in $|z-a|_p < R$.

For completeness, we mention also the following analogue of the Weierstrass approximation theorem.

Proposition 6.22 (Chernoff, Rasala and Waterhouse). Let F be a topological field and K be a compact subset of F. Then the polynomials are uniformly dense in the continuous F-valued functions on K.
(For the proof see Lemma 3 of Chernoff, Rasala and Waterhouse [11].)

CHAPTER 7

INTERPOLATION

1. The interpolation problem.

The interpolation problem investigated in this chapter is the p-adic analogue of what is known as Hermite's interpolation problem, which is the extension of the problems considered in section 1 of Chapter 6 to the case when the interpolation points are not all distinct. First, the existence of the interpolation polynomial will be established and then in section 2 different forms of this polynomial will be derived via divided differences. If the function to be approximated is analytic, then by using Schnirelman integrals we can obtain results similar to those in the complex case, as mentioned in Chapter 6, and this is done in section 3. Section 4 illustrates some applications of the results on interpolation in sections 1 to 3. In section 5 certain bounds on the interpolation polynomial and its coefficients will be obtained in various forms ready to be used in Chapter 8. These bounds are of importance in proving auxiliary results in the theory of transcendental numbers. The chapter ends up with similar results on interpolation by rational functions, instead of polynomials. Now we prove the existence theorem.

Theorem 7.1. Let $\omega_1,\ldots,\omega_m$ be m distinct points in Ω_p and $\rho(1),\ldots,\rho(m)$ be positive integers such that

$$\sum_{k=1}^{m} \rho(k) = n.$$

Let also f be a function defined at $\omega_1,\ldots,\omega_m$ with its derivatives at ω_k $(k=1,\ldots,m)$ up to the $(\rho(k)-1)$th order. Then there exists a unique polynomial $Q(z)$ of degree at most $n-1$ such that

$$Q^{(s)}(\omega_k) = f^{(s)}(\omega_k) \qquad (k=1,\ldots,m;\quad s=0,1,\ldots,\rho(k)-1)$$

Proof. Let us write

$$Q(z) = \sum_{i=0}^{n-1} q_i z^i .$$

To satisfy all the required conditions, we must have

$$\sum_{i=0}^{n-1} q_i \omega_k^i = f(\omega_k) \qquad (k=1,\ldots,m),$$

and

$$\sum_{i=s}^{n-1} \binom{i}{s-1}(s-1)!\; q_i \omega_k^{i-s} = f^{(s)}(\omega_k)$$

$$(s=1,\ldots,\rho(k)-1;\quad k=1,\ldots,m).$$

Here we have a system of n linear equations in n unknowns $q_0,\ldots,q_{n-1}$ and the determinant of this system is (see Gelfond [14] page 41)

$$\pm \prod_{k=1}^{m} \prod_{j=0}^{\rho(k)-1} \left\{ j! \prod_{k>s} (\omega_k-\omega_s)^{\rho(s)} \right\},$$

which is non-zero as all ω_k are distinct. Hence the system has unique solution $q_0,\ldots,q_{n-1}$ and the theorem is proved.

2. Divided differences and general formulae for interpolation polynomial.

We now introduce divided differences for a given function f and interpolation points $\eta_0,\ldots,\eta_{n-1}$ which are not necessarily distinct.

<u>Definition</u>. The <u>divided differences</u> $[\eta_0,\ldots,\eta_k; f]$ are defined by induction as follows. For $0 \leqslant k \leqslant n-1$, we define

$$[\eta_k; f] = f(\eta_k).$$

For $0 \leqslant k < k+r < n$, if $\eta_k \neq \eta_{k+r+1}$, we define

$$[\eta_k,\ldots,\eta_{k+r+1}; f] = \frac{[\eta_k,\ldots,\eta_{k+r}; f] - [\eta_{k+1},\ldots,\eta_{k+r+1}; f]}{\eta_k - \eta_{k+r+1}};$$

and if $\eta_k = \eta_{k+r+1}$, we replace η_{k+r+1} in the above quotient by η and define

$$[\eta_k,\ldots,\eta_{k+r+1}; f] = \lim_{\eta\to\eta_k} \frac{[\eta_k,\ldots,\eta_{k+r}; f] - [\eta_{k+1},\ldots,\eta_{k+r},\eta; f]}{\eta_k - \eta},$$

provided this limit exists.

We illustrate this definition with some examples, several of which will be used later.

<u>Example 7.2.1</u>. Let I^r $(r=0,1,2,\ldots)$ be the mappings

$$I^r : z \mapsto z^r .$$

Let $\eta_0,\eta_1,\ldots,\eta_{n-1}$ be as before. Then

$$[\eta_0; I^r] = \eta_0^r ,$$

$$[\eta_0,\eta_1; I^r] = \eta_0^{r-1} + \eta_0^{r-2}\eta_1 + \eta_0^{r-3}\eta_1^2 + \ldots + \eta_1^{r-1}.$$

In general, if $0 \leqslant k \leqslant r$, then

$$[\eta_0,\eta_1,\ldots,\eta_k; I^r] = \sum \eta_0^{s_0}\eta_1^{s_1} \ldots \eta_k^{s_k} ,$$

where the summation extends over all possible non-negative integers $s_0,\ldots,s_k$ such that

$$s_0 + s_1 + \ldots + s_k = r-k.$$

There are $\binom{r}{k}$ distinct terms in this summation. Therefore, if $\eta_0 = \eta_1 = \ldots = \eta_k = \eta$, and $0 \leqslant k \leqslant r$, then

$$[\eta_0,\ldots,\eta_k; I^r] = [\eta,\ldots,\eta; I^r] = \binom{r}{k} \eta^{r-k} = \frac{1}{k!}\left(D^k z^r\right)_{z=\eta}.$$

Also, in particular, for any $\eta_0, \eta_1, \ldots, \eta_r$,

$$[\eta_0, \eta_1, \ldots, \eta_r; I^r] = 1 ,$$

$$[\eta_0, \eta_1, \ldots, \eta_k; I^r] = 0 \qquad (k > r).$$

Example 7.2.2. If $\eta_0, \eta_1, \ldots, \eta_{n-1}$ as defined above are all distinct, then by expanding according to the definition of divided differences, we get

$$[\eta_0, \ldots, \eta_i; f] = \frac{[\eta_0, \ldots, \eta_{i-1}; f] - [\eta_1, \ldots, \eta_i; f]}{\eta_0 - \eta_i} \qquad (0 \leqslant i \leqslant n-1),$$

$$[\eta_0, \ldots, \eta_{i-1}; f] = \frac{[\eta_0, \ldots, \eta_{i-2}; f] - [\eta_1, \ldots, \eta_{i-1}; f]}{\eta_0 - \eta_{i-1}}$$

and so on. Hence

$$[\eta_0, \ldots, \eta_i; f] = \sum_{j=0}^{i} \frac{f(\eta_j)}{(\eta_j - \eta_0)\ldots(\eta_j - \eta_{j-1})(\eta_j - \eta_{j+1})\ldots(\eta_j - \eta_i)} .$$

In particular, for $\eta_0 = 0$, $\eta_1 = 1, \ldots, \eta_{n-1} = n-1$, this is the Mahler expansion (see Mahler [26])

$$[0, 1, \ldots, n-1; f] = \frac{1}{i!} \sum_{j=0}^{i} (-1)^j \binom{i}{j} f(i-j) .$$

Example 7.2.3. Let $\eta_0, \ldots, \eta_{n-1}$ be distinct elements in Ω_p; I^r be as in Example 7.2.1. By applying the result of Example 7.2.2 to

$$[\eta_0^{-1}, \ldots, \eta_i^{-1}; I^{r+i-1}] \quad \text{and} \quad [\eta_0, \ldots, \eta_i, I^{-r}] ,$$

we get

$$[\eta_0^{-1}, \ldots, \eta_i^{-1}; I^{r+i-1}] = (-1)^{i+1} \eta_0 \ldots \eta_i [\eta_0, \ldots, \eta_i; I^{-r}].$$

Example 7.2.4. Let $\eta_i \, (0 \leqslant i \leqslant n-1)$ be as before. If for some k, r, we have

$$\eta_k = \eta_{k+1} = \ldots = \eta_{k+r} = \eta$$

and ~~$f^{(r)}(\eta)$ exists,~~ f is analytic in $|z|_w < \rho$, where $|\eta|_w < \rho$, then

$$[\eta_k, \ldots, \eta_{k+r}; f] = [\eta, \ldots, \eta; f] = \frac{1}{r!} [D^r f(z)]_{z=\eta} .$$

Now we specify the set $\{\eta_0, \ldots, \eta_{n-1}\}$ so that we can proceed to say something about Theorem 7.1. Let $\omega_1, \omega_2, \ldots, \omega_m$ be m distinct elements in Ω_p. Consider the sequence

(7.1) $(\eta_0, \eta_1, \ldots, \eta_{n-1}) = (\omega_1, \ldots, \omega_1, \omega_2, \ldots, \omega_2, \ldots, \omega_m, \ldots, \omega_m)$

where ω_k $(1 \leqslant k \leqslant m)$ is repeated $\rho(k)$ times with

$$n = \sum_{k=1}^{m} \rho(k) .$$

The following lemma is basic for most of our subsequent work.

Lemma 7.2. Let $\eta_0, \ldots, \eta_{n-1}$, $\omega_1, \ldots, \omega_m$ be as just defined above. Let f and g be two p-adic functions. We have then

(7.2) $\qquad [\eta_0, \ldots, \eta_i; f] = [\eta_0, \ldots, \eta_i; g] \qquad (i = 0, 1, \ldots, n-1)$

if and only if

(7.3) $\qquad f^{(s)}(\omega_k) = g^{(s)}(\omega_k) \qquad (s = 0, 1, \ldots, \rho(k) - 1;$
$k = 1, \ldots, m).$

Proof. It is easily shown by induction that (7.2) holds if and only if

$$[\eta_k, \eta_{k+1}, \ldots, \eta_{k+r}; f] = [\eta_k, \eta_{k+1}, \ldots, \eta_{k+r}; g],$$

for all k, r such that

$$0 \leqslant k \leqslant k + r \leqslant n.$$

The equivalence of this with (7.3) can then be derived by using induction on r and Example 7.2.4.

To simplify the notation, we set up the following:

Definition. Let f, g be p-adic functions and let $\eta_0, \ldots, \eta_{n-1}$, $\omega_1, \ldots, \omega_m$ be as defined in (7.1) above.

We write

$$f \equiv g \pmod{\eta_0,\ldots,\eta_{n-1}}$$

if and only if (7.2) and hence (7.3) holds.

The next theorem allows us to write the unique polynomial Q in Theorem 7.1 in a simple form.

Theorem 7.3. Let $\eta_0,\ldots,\eta_{n-1}$, $\omega_1,\ldots,\omega_m$ be defined as in (7.1) and let f and Q be as in Theorem 7.1. Then Q can be represented by Newton's interpolation formula

$$(7.4) \qquad Q(z) = \sum_{i=0}^{n-1} [\eta_0,\ldots,\eta_i; f]\,(z-\eta_0)\ldots(z-\eta_{i-1}).$$

Proof. Let Q satisfy (7.4). It is then easily checked by induction that

$$[\eta_0,\ldots,\eta_i; Q] = [\eta_0,\ldots,\eta_i; f] \quad (0 \leqslant i \leqslant n-1)$$

The result now follows immediately from Theorem 7.1 and Lemma 7.2.

Theorem 7.4. Let $\eta_0,\ldots,\eta_{n-1}$, $\omega_1,\ldots,\omega_m,f,Q$ be as in Theorem 7.3. Then

$$f(z) = Q(z) + [z,\eta_0,\ldots,\eta_{n-1}; f](z-\eta_0)\ldots(z-\eta_{n-1}).$$

That is, the error $f(z) - Q(z)$ is

$$[z,\eta_0,\ldots,\eta_{n-1}; f]\,(z-\eta_0)\ldots(z-\eta_{n-1}).$$

Proof. Consider an element z distinct from all η_i $(0 \leqslant i \leqslant n-1)$. By expanding the divided difference $[z,\eta_0,\ldots,\eta_{n-1}; f]$, we obtain

$$[z,\eta_0,\ldots,\eta_{n-1}; f] = \frac{f(z)}{(z-\eta_0)\ldots(z-\eta_{n-1})} - \frac{[\eta_0; f]}{(z-\eta_0)\ldots(z-\eta_{n-1})} - \frac{[\eta_0,\eta_1; f]}{(z-\eta_1)\ldots(z-\eta_{n-1})} - \ldots - \frac{[\eta_0,\eta_1,\ldots,\eta_{n-1}; f]}{z-\eta_{n-1}}.$$

Hence, by (7.4) we have

$$[z,\eta_0,\ldots,\eta_{n-1}; f]\,(z-\eta_0)\ldots(z-\eta_{n-1}) = f(z) - Q(z).$$

If $z = \eta_i$ for some i, this last equality also holds and so the theorem follows.

Theorem 7.5. Let the hypotheses be as in Theorem 7.3. If all η_i $(0 \leq i \leq n-1)$ are distinct, then Q can be represented by Lagrange's formula

$$Q(z) = \sum_{i=0}^{n-1} \frac{f(\eta_i)\varphi(z)}{(z-\eta_i)\varphi'(\eta_i)}, \tag{7.5}$$

where

$$\varphi(z) = (z-\eta_0)\ldots(z-\eta_{n-1}).$$

Proof. As in the proof of Theorem 7.4, if we expand $[z,\eta_0,\ldots,\eta_{n-1}; f]$ using Example 7.2.2, we get

$$[z,\eta_0,\ldots,\eta_{n-1}; f] = \frac{f(z)}{(z-\eta_0)\ldots(z-\eta_{n-1})} +$$

$$+ \sum_{i=0}^{n-1} \frac{f(\eta_i)}{(\eta_i-z)(\eta_i-\eta_0)\ldots(\eta_i-\eta_{i-1})(\eta_i-\eta_{i+1})\ldots(\eta_i-\eta_{n-1})}$$

$$= \frac{f(z)}{\varphi(z)} + \sum_{i=0}^{n-1} \frac{f(\eta_i)}{(z-\eta_i)\varphi'(\eta_i)},$$

Thus

$$f(z) = \sum_{i=0}^{n-1} \frac{f(\eta_i)\varphi(z)}{(z-\eta_i)\varphi'(\eta_i)} + [z,\eta_0,\ldots,\eta_{n-1}; f]\,\varphi(z).$$

By the uniqueness of Q and comparing with Theorem 7.4, we obtain the desired result.

3. Interpolation of analytic functions.

If the function f described in section 2 is analytic in $|z|_p \leq R$ for some positive real number R, then by using Schnirelman integrals we obtain

Theorem 7.6. (i) Let $\rho \in \Omega_p$ be such that

$$|\rho|_p \leq R,$$

and let $\eta_0,\ldots,\eta_{n-1}$ be such that

$$|\eta_i|_p < |\rho|_p \qquad (0 \leq i \leq n-1).$$

Suppose f is analytic in $|z|_p \leqslant R$, then

(7.6) $$[\eta_0,\eta_1,\ldots,\eta_i;\, f\,] = \int_{o,\rho} \frac{f(z)zdz}{(z-\eta_0)\ldots(z-\eta_i)}$$

$(0 \leqslant i \leqslant n-1)$.

(ii) If $|\eta_i|_p \leqslant R$ for $i = 0,\ldots,n-1$ and the power series expansion of f as above is

$$f(z) = \sum_{r=0}^{\infty} A_r z^r \qquad (|z|_p \leqslant R),$$

then also

$$[\eta_0,\eta_1,\ldots,\eta_i;\, f\,] = \sum_{r=i}^{\infty} A_r\, [\eta_0,\eta_1,\ldots,\eta_i; I^r]$$

$(0 \leqslant i \leqslant n-1)$,

where I^r are as defined in Example 7.2.1.

Proof. (i) For $i = 0$, (7.6) holds by Proposition 6.13 (p-adic Cauchy's integral formula). It is then easily proved for $i > 0$ by induction, using the fact that, whether or not $\eta_0 = \eta_{i+1}$, we have

$$\int_{o,\rho} \frac{f(z)zdz}{(z-\eta_0)\ldots(z-\eta_i)} - \int_{o,\rho} \frac{f(z)zdz}{(z-\eta_1)\ldots(z-\eta_{i+1})}$$

$$= (\eta_0-\eta_{i+1}) \int_{o,\rho} \frac{f(z)zdz}{(z-\eta_0)\ldots(z-\eta_{i+1})}\,.$$

(ii) This is easily proved by applying the definition of divided differences directly to the series and using uniform convergence.

Now we come to the main theorem of this chapter.

Theorem 7.7. Let $f,\omega_1,\ldots,\omega_m$, Q be as in Theorem 7.1. Then Q can be represented by Hermite's interpolation formula

$$(7.7) \qquad Q(z) = \sum_{k=1}^{m} \sum_{s=0}^{\rho(k)-1} \sum_{i=0}^{\rho(k)-s-1} \frac{f^{(s)}(\omega_k)}{s!\big((\rho(k)-s-1-i)!\big)} \left[D^{\rho(k)-s-1-i}\left(\frac{(u-\omega_k)^{\rho(k)}}{\varphi(z)}\right)\right]_{u=\omega_k} \frac{\varphi(z)}{(z-\omega_k)^{i+1}},$$

where

$$\varphi(z) = (z-\omega_1)^{\rho(1)} \cdots (z-\omega_m)^{\rho(m)}.$$

Moreover if f is analytic in $|z|_p \leqslant R$ and $\rho \in \Omega_p$ is such that

$$|\omega_i|_p < |\rho|_p \leqslant R \qquad (0 \leqslant i \leqslant n-1),$$

then

$$(7.8) \qquad Q(z) = -\varphi(z) \sum_{k=1}^{m} \int_{\omega_k, t} \frac{(u-\omega_k)^{\rho(k)} f(u)(u-\omega_k)\,du}{(u-z)\ \varphi(u)} \qquad (|z|_p < |\rho|_p),$$

where $t \in \Omega_p \sim \{0\}$ is such that $|\omega_k-\omega_j|_p > |t|_p \quad (k \neq j)$ (as seen, for example, in Proposition 6.16). We also have the error

$$(7.9) \qquad f(z) - Q(z) = \int_{0,\rho} \frac{\varphi(z) f(u)\,u\,du}{(u-z)\varphi(u)} \qquad (|z|_p < |\rho|_p).$$

<u>Proof</u>. If Hermite's formula (7.7) holds for f analytic on $|z|_p \leqslant R$, then in particular it applies to the interpolation polynomial for any f. Hence we may suppose that f is analytic on $|z|_p \leqslant R$.

Let $\eta_0, \eta_1, \ldots, \eta_{n-1}$ be as in (7.1). Then by Theorem 7.4 and equation (7.6), since $\varphi(z) = (z-\eta_0)\ldots(z-\eta_{n-1})$,

$$\begin{aligned} f(z) - Q(z) &= \varphi(z)\ [z, \eta_0, \ldots, \eta_{n-1}; f\,] \\ &= \int_{0,\rho} \frac{\varphi(z) f(u)\,u\,du}{(u-z)\varphi(u)} = I \end{aligned} \qquad (|z|_p < |\rho|_p),$$

say. Thus we have proved (7.9). Now we derive both expressions for $Q(z)$ from this.

Write

$$\psi(u) = \frac{f(u)}{(u-z)\varphi(u)} \quad .$$

Then by the residue theorem (Proposition 6.16), for $z = \omega_i$ $(0 \leqslant i \leqslant n-1)$, $|z|_p < |\rho|_p$,

$$I = \Big(\mathrm{res}(\psi;z) + \sum_{k=1}^{m} \mathrm{res}(\psi;\omega_k)\Big)\varphi(z) .$$

Since $\varphi(z)\mathrm{res}(\psi;z)$ is $f(z)$ by directly computing the residue at z, it then follows that

$$Q(z) = -\varphi(z) \sum_{k=1}^{m} \mathrm{res}(\psi;\omega_k) \quad ,$$

and this yields the expression (7.8) for $Q(z)$. Now we must compute the residues.

Since the power of $(u-\omega_k)$ dividing $\varphi(u)$ is exactly $\rho(k)$, it follows from Proposition 6.13 (Cauchy's integral formula) that the residue of ψ at ω_k is

$$\frac{1}{(\rho(k)-1)!}\left[D^{\rho(k)-1}\left(\frac{(u-\omega_k)^{\rho(k)} f(u)}{(u-z)\varphi(u)}\right)\right]_{u=\omega_k}$$

$$= \sum_{s=0}^{\rho(k)-1} \frac{f^{(s)}(\omega_k)}{s!\,(\rho(k)-s-1)!}\left[D^{\rho(k)-s-1}\left(\frac{(u-\omega_k)^{\rho(k)}}{(u-z)\varphi(u)}\right)\right]_{u=\omega_k}$$

$$= \sum_{s=0}^{\rho(k)-1} \frac{f^{(s)}(\omega_k)}{s!} \sum_{i=0}^{\rho(k)-s-1} \frac{-1}{(\rho(k)-s-1)!}$$

$$\left[D^{\rho(k)-s-1-i}\left(\frac{(u-\omega_k)^{\rho(k)}}{\varphi(u)}\right)\right]_{u=\omega_k} \frac{1}{(z-\omega_k)^{i+1}} \quad .$$

Combining all these results, we see that the equation (7.8) holds for $|z|_p \leqslant |\rho|_p$ and hence for all z, since both sides of the equation are polynomials.

We note here that the work of van der Poorten [33] was based on the following related form for Q.

$$Q(z) = \sum_{k=1}^{m} \sum_{s=0}^{\rho(k)-1} E^{(s)}(\omega_k) \left\{ \prod_{\substack{i=1\\ i\neq k}}^{m} \left(\frac{z-\omega_i}{\omega_k-\omega_i}\right)^{\rho(i)-1} \frac{(z-\omega_i)^s}{s!} \right. .$$

$$\left. \sum_{\lambda} \frac{\prod_{r=s}^{\rho(k)-1} \left(\frac{\partial}{\partial\omega_k}\right)^{\lambda} \left\{(z-\omega_k)\prod_{\substack{j=1\\ j\neq k}}^{m}(\omega_k-\omega_j)^{\rho(j)-1}\right\}(-1)^{\max\{0,\lambda(r)-1\}}}{\lambda(r)!\prod_{\substack{j=1\\ j\neq k}}^{m}(\omega_k-\omega_j)^{\rho(j)-1}} \right\}$$

where the last sum is over all non-negative integer sets $\lambda(s),\ldots,\lambda(\rho(k)-1)$ with sum $\rho(k)-s+1$ and such that $\lambda(r)\leqslant r-s+1$ and such that $\lambda(\rho(k)-1)\geqslant 1$ (if $s-1=\rho(k)$, the sum is of course empty).

We conclude this section by looking at the relationship between analytic functions and interpolation series in Ω_p (which is much simpler than the corresponding relationship in $\mathbb{Q}_p$, as can be seen from Mahler [26]).

Theorem 7.8. Let (η_m) be a sequence of (not necessarily distinct) points in Ω_p such that

$$|\eta_m|_p \leqslant R \qquad (m=0,1,2,\ldots).$$

(i) If f is analytic in $|z|_p\leqslant R$, then f is represented by the interpolation series

$$f(z) = \sum_{i=0}^{\infty} [\eta_0,\ldots,\eta_i;\, f\,](z-\eta_0)\ldots(z-\eta_{n-1}) \qquad (|z|_p\leqslant R),$$

and this series is uniformly convergent on $|z|_p\leqslant R$.

(ii) If f has a representation

$$f(z) = \sum_{i=0}^{\infty} a_i(z-\eta_0)\ldots(z-\eta_{i-1}) \qquad (|z|_p\leqslant R),$$

where the series is uniformly convergent on $|z|_p\leqslant R$, then f is analytic in $|z|_p < R$.

Proof. (i) Suppose

$$f(z) = \sum_{i=0}^{\infty} A_i z^i \qquad (|z|_p\leqslant R),$$

and let Q_m be the unique polynomial of degree at most $m-1$ such that

$$Q_m \equiv f \pmod{\eta_0,\ldots,\eta_{m-1}}.$$

By Theorem 7.4, Theorem 7.6 (ii) and Example 7.2.1, we have, for $|z|_p \leqslant R$,

$$|f(z)-Q_m(z)|_p = |[z,\eta_0,\ldots,\eta_{m-1};f]\,(z-\eta_0)\ldots(z-\eta_{m-1})|_p$$

$$\leqslant R^m \Big| \sum_{r=m}^{\infty} A_r[z,\eta_0,\ldots,\eta_{m-1};I^r]\Big|_p$$

$$\leqslant R^m \max_{r\geqslant m} R^{r-m-1}|A_r|_p = R^{-1}\max_{r\geqslant m} R^r|A_r|_p\ ,$$

which tends to 0 as $m\to\infty$. Thus $Q_m \to f$ uniformly on $|z|_p \leqslant R$ and the result follows from Newton's formula for Q_m (Theorem 7.3).

(ii) This is an immediate consequence of Proposition 6.21 on uniformly convergence sequence of analytic functions.

Corollary. If f is analytic in $|z|_p \leqslant R$ and is not identically zero, then it has at most a finite number of zeros in $|z|_p \leqslant R$.

Proof. If f has infinitely many zeros (counted with multiplicity) in $|z|_p \leqslant R$, we can apply (i) above with (η_m) as the sequence of zeros. This implies that all divided differences vanish and hence f is identically zero.

We note in particular that if the points η_m are distinct and

$$a_m(\eta_m-\eta_0)(\eta_m-\eta_1)\ldots(\eta_m-\eta_{m-1}) \to 0 \qquad (n\to\infty),$$

and

$$|(z-\eta_0)\ldots(z-\eta_{m-1})|_p \leqslant |(\eta_m-\eta_0)\ldots(\eta_m-\eta_{m-1})|_p \quad (|z|_p\leqslant R),$$

then the series in (ii) is uniformly convergent on $|z|_p \leqslant R$ and is identical with the series in (i). This case corresponds to the situation considered in $\mathcal{Q}_p$ by Mahler [26] and in local fields by Amice [4], and it is easily shown that here, too, the polynomials Q_m are best approximations.

4. Some consequences of interpolation.

In this section, some approximation results are proved to illustrate the use of theorems proved in sections 1 to 3. (Compare with Lemma 1 and Theorem 1, page 310 of Walsh [43].)

Consequence 7.4.1. Let R be a positive real number and $\eta_0, \eta_1, \ldots, \eta_{n-1}$ be distinct elements of Ω_p such that

$$|\eta_i|_p \leqslant R \qquad (0 \leqslant i \leqslant n-1).$$

Then there exists a real constant K such that if

$$|v_i|_p \leqslant v \qquad (0 \leqslant i \leqslant n-1),$$

then

$$|Q(z)|_p \leqslant Kv \qquad (|z|_p \leqslant R),$$

where $Q(z)$ is the unique polynomial of degree at most $n-1$ which takes on the values v_i at the points η_i $(0 \leqslant i \leqslant n-1)$.

Proof. From Lagrange's formula (7.5), we have

$$Q(z) = \sum_{i=0}^{n-1} \frac{v_i \, \varphi(z)}{(z-\eta_i)\varphi'(\eta_i)},$$

where $\varphi(z) = (z-\eta_0)\ldots(z-\eta_{n-1})$.

Since $Q(z)$ is analytic for $|z|_p \leqslant R$, then

$$|Q(z)|_p \leqslant \max_{0 \leqslant i \leqslant n-1} \left| v_i \frac{\varphi(z)}{(z-\eta_i)\varphi'(\eta_i)} \right|_p$$

$$\leqslant Kv,$$

where

$$K = \max_{|z|_p \leqslant R} \max_{0 \leqslant i \leqslant n-1} \left| \frac{\varphi(z)}{(z-\eta_i)\varphi'(\eta_i)} \right| .$$

Consequence 7.4.2. Let S be a bounded subset of Ω_p and let $\eta_0,\ldots,\eta_{n-1}$ be distinct points of Ω_p (not necessarily in S), and let f be defined on S and at $\eta_0,\ldots,\eta_{n-1}$. If f is uniformly approximable on S by polynomials, then it is uniformly approximable on S by polynomials Q such that

$$Q \equiv f \pmod{\eta_0,\ldots,\eta_{n-1}}.$$

Proof. Take an $\varepsilon > 0$ and take $R > 0$ such that $|z|_p \leqslant R$ for all z in S and $|\eta_i|_p \leqslant R$ for all i. Let K be the constant in Consequence 7.4.1 corresponding to this value of R. Then there is a polynomial P such that

$$|f(z) - P(z)|_p \leqslant \varepsilon/K \qquad (z \in S).$$

Now let G be the unique polynomial of degree at most $n-1$ satisfying

$$G \equiv f - P \pmod{\eta_0,\ldots,\eta_{n-1}}.$$

Define the polynomial Q by

$$Q(z) = P(z) + G(z).$$

Clearly, Q satisfies our requirements, that is

$$Q \equiv f \pmod{\eta_0,\ldots,\eta_{n-1}}$$

and by the strong triangle inequality and Consequence 7.4.1, for z in S we have

$$\begin{aligned} |f(z) - Q(z)|_p &\leqslant \max\left(|f(z) - P(z)|_p, |G(z)|_p\right) \\ &\leqslant \max(\varepsilon/K, K\cdot\varepsilon/K). \end{aligned}$$

In particular, it also follows from Proposition 6.22 that if S is compact and f is continuous on S, then f is uniformly approximable by polynomials Q interpolating at $\eta_0,\ldots,\eta_{n-1}$.

Of course, Consequence 7.4.2 yields nothing beyond what we already know from Proposition 6.21 and Theorem 7.8 if S is a disc $|z|_p \leqslant R$ and η_i is in S for all i. We now apply it with the η_i outside S to obtain an analogue of Mittag-Leffler's theorem. Our hypothesis is stronger than in the classical case because the disc $|z|_p \leqslant 1$ is not compact.

Consequence 7.4.3 (Mittag-Leffler Theorem; compare Walsh [43; pages 312-313]). Let (η_n) be a sequence of distinct elements in $|z|_p \leqslant 1$, and suppose that for R such that $0 < R < 1$ at most a finite number of these elements are in $|z|_p \leqslant R$. Let (v_k) be a given sequence in Ω_p. Then there exists a function g analytic in $|z|_p < 1$ such that

$$g(\eta_k) = v_k \qquad (k = 0,1,2,\ldots)$$

Proof. Without loss of generality, let the points η_k be as arranged that

$$|\eta_0|_p \leqslant |\eta_1|_p \leqslant |\eta_2|_p \leqslant \ldots \quad \to 1$$

Denote by ℓ_{k-1} the largest of the numbers $|\eta_0|_p, |\eta_1|_p, \ldots, |\eta_{k-1}|_p$ which is actually less that $|\eta_k|_p$, with $\ell_0 = |\eta_0|_p$. Now choose

$$Q_0(z) \equiv v_0 \qquad (|z|_p \leqslant 1).$$

By applying Consequence 7.4.2 with S as the disc $|z|_p \leqslant \ell_0$, $n=1$, $\eta_0 \in S$, $\eta_1 \notin S$, and define the function f by

$$f(z) = 0 \qquad (z \in S),$$

$$f(\eta_1) = v_1 - v_0,$$

we can obtain a polynomial Q_1 satisfying

$$Q_1 \equiv f \pmod{\eta_0, \eta_1},$$

$$|Q_1(z)|_p < p^{-1} \qquad (z \in S).$$

By repeating this process, in general, we obtain a polynomial Q_k $(k > 1)$ satisfying

$$Q_k(\eta_k) = v_k - Q_{k-1}(\eta_k) - \ldots - Q_0(\eta_k) ,$$

$$Q_k(\eta_0) = Q_k(\eta_1) = \ldots = Q_k(\eta_{k-1}) = 0 ,$$

$$|Q_k(z)|_p < p^{-k} \qquad (|z|_p \leqslant \ell_{k-1}).$$

$\Sigma Q_k(z)$ converges uniformly on $|z|_p \leqslant R$ for any R such that $0 < R < 1$ (because $R \leqslant \ell_{k-1}$ for some k) and hence by Proposition 6.21, it is analytic in $|z|_p < 1$.

5. Bounds on the interpolation polynomials and its coefficients.

With certain applications in Chapter 8 in mind, some accurate bounds on the interpolation polynomials and its coefficients will be derived in this section.

First, the following set up will be used throughout this section:

I^r is as defined in Example 7.2.1,

$\eta_0, \eta_1, \ldots, \eta_{n-1}$ denotes n elements of Ω_p, not necessarily distinct,

$\omega_1, \ldots, \omega_m$ denote m distinct elements of Ω_p,

$\rho(1), \ldots, \rho(m)$ denote m non-negative integers.

Lemma 7.9. If $P = P(r;z)$ is the unique polynomial of degree at most $n-1$ such that

$$P \equiv I^r \pmod{\eta_0,\ldots,\eta_{n-1}},$$

then

$$P(r;z) = \sum_{k=0}^{n-1} c_{rk} z^k \quad ,$$

where

(7.10)

$$c_{rk} = [\eta_0,\eta_1,\ldots,\eta_k;I^r] - [\eta_0,\ldots,\eta_{k+1};I^r]S_1(\eta_0,\ldots,\eta_{k+1}) + \ldots$$
$$+ (-1)^{n-k-1}[\eta_0,\eta_1,\ldots,\eta_{n-1};I^r]S_{n-k-1}(\eta_0,\ldots,\eta_{n-1}),$$

with

$$\begin{aligned} S_i(\eta_0,\eta_1,\ldots,\eta_{k+i}) &= \eta_0\eta_1\ldots\eta_i + \ldots \qquad (1 \leqslant i \leqslant n-k-1) \\ &= i^{th} \text{ elementary symmetric} \\ &\quad \text{function of } (\eta_0,\ldots,\eta_{k+i}). \end{aligned}$$

Proof. From Theorem 7.3, we have

$$P(r;z) = \sum_{i=0}^{n-1} [\eta_0,\ldots,\eta_i;I^r]\ (z-\eta_0)\ldots(z-\eta_{i-1}).$$

If we also write

$$P(r;z) = \sum_{k=0}^{n-1} c_{rk} z^k \ ,$$

the result follows by equating coefficients of z^k $(0 \leqslant k \leqslant n-1)$.

Since I^r itself satisfies the requirements for P if $0 \leqslant r < n$, we have

$$\begin{aligned} &P(0;z) = 1, \\ (7.11) \qquad &P(1;z) = z, \\ &\quad \vdots \\ &P(n-1;z) = z^{n-1} \end{aligned}$$

Theorem 7.10. Let $\eta_0,\ldots,\eta_{n-1}$, R and f be as above with

$$|\eta_i|_p \leqslant R \qquad (0 \leqslant i \leqslant n-1),$$

$$f(z) = \sum_{r=0}^{\infty} A_r z^r \qquad (|z|_p \leqslant R).$$

If Q is the unique polynomial of degree at most $n-1$ such that

$$Q \equiv f \pmod{\eta_0, \eta_1, \ldots, \eta_{n-1}},$$

then

$$Q(z) = \sum_{r=0}^{\infty} A_r P(r;z), \tag{7.12}$$

where $P(r;z)$ are as defined in Lemma 7.9. More precisely

$$Q(z) = A_0 + A_1 z + \ldots + A_{n-1} z^{n-1} + \sum_{r=n}^{\infty} A_r P(r;z).$$

Proof. By Theorems 7.3 and 7.6,

$$Q(z) = \sum_{i=0}^{n-1} [\eta_0, \ldots, \eta_i; f] \, (z-\eta_0) \ldots (z-\eta_{i-1})$$

$$= \sum_{i=0}^{n-1} \sum_{r=0}^{\infty} A_r [\eta_0, \eta_1, \ldots, \eta_i; I^r] \, (z-\eta_0) \ldots (z-\eta_i)$$

$$= \sum_{r=0}^{\infty} A_r P(r;z),$$

The second assertion of the theorem follows from the formulae in (7.21).

Now we are in a position to obtain upper bounds for the coefficients of Q described in Theorem 7.10.

Theorem 7.11. Let Q as in Theorem 7.10 be written as

$$Q(z) = \sum_{k=0}^{n-1} q_k z^k.$$

Then

$$|q_k|_p \leqslant \max\left(|A_k|_p, \max_{r \geqslant k+1} |A_r c_{rk}|_p\right), \tag{7.13}$$

where c_{rk} are as defined in (7.10). Also, there is a stronger bound

$$|q_k|_p \leqslant \max\left(|A_k|_p, \max_{r \geqslant n} |A_r c_{rk}|_p\right). \tag{7.14}$$

Proof. (7.13) follows by equating coefficients of z^k with (7.12) as well as using (7.10) and the strong-triangle inequality. For the stronger form (7.14) the use of (7.11) is also made.

The next theorems estimate some bounds of a particular polynomial that will be used in the latter part of Chapter 8.

Theorem 7.12. Let $\omega_1, \ldots, \omega_m$, $\rho(1), \ldots, \rho(m)$ be as defined at the beginning of this section. Let also N, M be two integers satisfying

$$1 \leqslant M \leqslant m \;, \qquad 0 \leqslant N \leqslant \rho(M) - 1.$$

If $Q_{MN}(z)$ is the unique polynomial of degree at most $n-1$ such that

$$Q_{MN}^{(\mu)}(\omega_\nu) = \begin{cases} 1 & (\mu = N, \ \nu = M) \\ 0 & (\mu \neq N, \ \nu \neq M, \ 0 \leqslant \mu \leqslant \rho(\nu) - 1, \ 1 \leqslant \nu \leqslant m), \end{cases}$$

then

$$|N!Q_{MN}(z)|_p \leqslant |\varphi(z)|_p \; |\rho|_p^{N+1} \max_{|u-\omega_M|_p = |\rho|_p} |(u-z)\varphi(u)|_p^{-1},$$

where $\varphi(z) = (z-\omega_1)^{\rho(1)} \ldots (z-\omega_m)^{\rho(m)}$, and $\rho \in \Omega_p$ such that

$$|\omega_i - \omega_M|_p > |\rho|_p \qquad (i \neq M, \ i = 1, \ldots, m).$$

Proof. By applying (7.7) of Theorem 7.7 to Q_{MN} and using the hypotheses on Q_{MN}, we obtain

$$Q_{MN}(z) = \frac{1}{(\rho(M)-N-1)!N!} \left[D^{\rho(M)-N-1}\left(\frac{(u-\omega_M)^{\rho(M)}}{(u-z)\varphi(u)} \right) \right]_{u=\omega_M} \varphi(z) .$$

Now by Proposition 6.13 (Cauchy's integral formula), it follows that

$$Q_{MN}(z) = \frac{\varphi(z)}{N!} \int_{\omega_M, \rho} \frac{(u-\omega_M)^{\rho(M)} (u-\omega_M) du}{(u-z)\varphi(u)(u-\omega_M)^{\rho(M)-N}} \;,$$

and hence by Proposition 6.11,

$$|N!Q_{MN}(z)|_p \leqslant |\varphi(z)|_p |\rho|_p^{N+1} \max_{|u-\omega_M|_p = |\rho|_p} |(u-z)\varphi(u)|_p^{-1} .$$

6. Interpolation by rational functions.

As in the case of interpolation by polynomials, some similar results can also be obtained if instead we interpolate by means of rational functions. In this section, such results will be given (compare with Theorem 1 page 184 and Theorem 2 page 186 of Walsh [43]).

Theorem 7.13. Let $\alpha_0,\ldots,\alpha_{n-1}$ be points in Ω_p. Let $v_0,\ldots,v_{n-1}$ be n given values in Ω_p and also let $\eta_0,\eta_1,\ldots,\eta_{n-1}$ be n distinct points in Ω_p, distinct also from all $\alpha_i (0 \leq i \leq n-1)$. Then there exists a unique rational function of the form

$$F(z) = \frac{b_{n-1}z^{n-1}+b_{n-2}z^{n-2}+\ldots + b_0}{(z-\alpha_0)(z-\alpha_1)\ \ldots\ (z-\alpha_{n-1})} \qquad (b_i \in \Omega_p;\ i=0,\ldots,n-1),$$

which takes the values v_i at the points z_i $(0 \leq i \leq n-1)$.

Proof. The proof is analogous to that of Theorem 7.1. The only difference is that now the determinant of the system is

$$\left(\prod_{s=0}^{n-1}\prod_{k=0}^{n-1}(\eta_s-\alpha_k)^{-1}\right)\left(\prod_{0\leq j<i\leq n-1}(\eta_i-\eta_j)\right)$$

which does not vanish according to the hypotheses of the theorem.

Theorem 7.14 (Lagrange's formula). Let the hypotheses be the same as in Theorem 7.13. Then we have

$$F(z) = \sum_{i=0}^{n-1}\frac{v_i\Psi(z)}{(z-\eta_i)\Psi'(\eta_i)} ,$$

where $$\Psi(z) = \frac{(z-\eta_0)\ldots(z-\eta_n)}{(z-\alpha_0)\ldots(z-\alpha_n)} .$$

If $f(z)$ is analytic in $|z|_p \leq R$ and $\rho \in \Omega_p$ is such that

$$|\eta_i|_p < |\rho|_p \leq R \qquad (0 \leq i \leq n-1),$$

then we also have

$$[\eta_0,\eta_1,\ldots,\eta_i;f] = \int_{0,\rho} \frac{f(u)udu}{\Psi(u)} ,$$

and the error term of the interpolation is

$$f(z) - F(z) = [z,\eta_0,\ldots,\eta_{n-1}]\ \Psi(z)$$

$$= \int_{0,\rho} \frac{\Psi(z)f(u)udu}{\Psi(u)(u-z)} \qquad (|z|_p < |\rho|_p)$$

Proof. The proof follows the lines of those in Theorems 7.5 and 7.6. In fact, it is simpler and similar to Example 7.2.2 due to the fact that all η_i $(0 \leqslant i \leqslant n-1)$ are distinct.

Theorems 7.13 and 7.14 can also be used to obtain analogues of Consequences 7.4.1 and 7.4.2 with rational functions in place of polynomials, corresponding to Lemma 2 and Theorem 3 page 313 of Walsh [43].

CHAPTER 8

APPLICATIONS

1. Introduction.

In this chapter some of the interpolation results of Chapter 7 will be applied to obtain p-adic analogues of number theoretic results similar to those mentioned in section 2 of Chapter 6. In section 2 p-adic analogues of two lemmas in Balkema and Tijdeman [7] will be proved and will be used to derive similar p-adic results of Turan's theorems (Theorems 6.2 and 6.3). Section 3 deals with p-adic exponential polynomials. First different estimates on the size of such polynomials will be derived and will then be employed to prove p-adic analogues of Theorem 6.1. The best results so far obtained in this direction are those in van der Poorten [33], as described in section 3 of Chapter 6, but his approach is different. My estimates of the number of zeros are close to his but not quite the same. Finally in section 4 I shall obtain a bound on the coefficients of exponential polynomials.

The approach used here is suggested by that of Shorey [38]. However, my results will be stronger owing to a better bound on the exponential polynomial. The only interpolation version used by van der Poorten [33] is the Hermite formula mentioned at the end of Theorem 7.7. Here I shall mainly use the version established in terms of divided differences (section 2 of Chapter 7) and Schnirelman integral (section 3 of Chapter 7). This approach simplifies the problem considerably. In fact the ideas renders a number of simplifications to the work of Balkema and Tijdeman in the classical case [7]; in particular their majorisation technique can be avoided. In the classical case the crux of the problem is to effectively estimate

$$[\eta_0, \ldots, \eta_n; f]$$

where f is an analytic function in $|z| \leqslant R$, that is,

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \qquad (a_0, a_1, \ldots \geqslant 0;\ |z| \leqslant R),$$

and for some constant η

$$|\eta_i| \leqslant \eta \qquad (i = 0, 1, \ldots, n).$$

Applying a result similar to Theorem 7.6 in Chapter 7, it can be shown that

$$|[\eta_0, \ldots, \eta_n; f]| = |\sum_{n=0}^{\infty} a_n [\eta_0, \ldots, \eta_n; I^r]| \leqslant |\sum_{n=0}^{\infty} a_n [\eta, \ldots, \eta; I^r]|$$

and thus

$$|[\eta_0, \ldots, \eta_n; f]| \leqslant |f^{(n)}(\eta)|/|n!| .$$

However, a corresponding result does not apply in the p-adic case because it can happen that $|\eta_i|_p \leqslant \eta$ $(i = 0, \ldots, n)$ but

$$|[\eta_0, \ldots, \eta_n; I^s]|_p = \eta^{s-n} > \left|\binom{s}{n}\right|_p \eta^{s-n} .$$

(See Example 7.2.1.) Thus some of the difficulties in the p-adic case are different form those in the classical case.

2. p-adic Turan's theorems.

Before turning to the main theorems of this section, we shall require the following lemma one part of which is proved in Shorey [38].

Lemma 8.1. Let $Q(z) = \sum_{k=0}^{n} q_k z^k$ be a p-adic polynomial. Then for any two sequences $\eta_0, \eta_1, \ldots, \eta_r$ and $b_0, b_1, \ldots, b_r$ of numbers in Ω_p, we have

$$(8.1) \qquad \left|\sum_{k=0}^{r} b_k Q(\eta_k)\right|_p \leq \left(\max_{0\leq h\leq n}|q_h|_p\right)\left(\max_{0\leq i\leq n}\left|\sum_{k=0}^{r} b_k \eta_k^i\right|_p\right) .$$

Furthermore, for $r = n$ and f any p-adic function, if Q is such that

$$Q \equiv f \pmod{\eta_0, \ldots, \eta_n},$$

then we have

$$(8.2) \qquad \left|\sum_{k=0}^{n} b_k f(\eta_k)\right| \leq \left(\max_{0\leq h\leq n}|q_h|_p\right)\left(\max_{0\leq i\leq n}\left|\sum_{k=0}^{n} b_k \eta_k^i\right|_p\right) .$$

Proof. To prove (8.1). By the strong triangle inequality we have

$$\left|\sum_{k=0}^{r} b_k Q(\eta_k)\right|_p = \left|\sum_{h=0}^{n}\sum_{k=0}^{r} b_k q_h \eta_k^h\right|_p \leq \max_{0\leq h\leq n}|q_h|_p \left|\sum_{k=0}^{r} b_k \eta_k^h\right|_p$$

$$\leq \left(\max_{0\leq h\leq n}|q_h|_p\right)\left(\max_{0\leq i\leq n}\left|\sum_{k=0}^{r} b_k \eta_k^i\right|_p\right) .$$

To prove (8.2) we simply note that for $r = n$,

$$Q(\eta_k) = f(\eta_k) \qquad (k = 0, 1, \ldots, n),$$

and substituting $Q(\eta_k)$ by $f(\eta_k)$, the result follows.

Theorem 8.2 (p-adic analogue of Turan's first main theorem). Let m, n be two non-negative integers with $n \geq 1$. Also let $b_0, \ldots, b_n$ and $\eta_0, \ldots, \eta_n$ be two sequences of numbers in Ω_p and $\eta_i (0 \leq i \leq n)$ be distinct. Then there exists an integer ν with $m+1 \leq \nu \leq m+n$ such that

$$\left|\sum_{k=0}^{n} b_k \eta_k^\nu\right|_p \geq \left|\sum_{k=0}^{n} b_k\right|_p \min_{0\leq i\leq n}|\eta_i|_p^\nu .$$

Proof. We may suppose without loss of generality that

$$\min_{0\leq i\leq n}|\eta_i|_p = 1 .$$

Thus we show that there exists an integer ν with $m+1 \leq \nu \leq m+n$ such that

$$\left|\sum_{k=0}^{n} b_k \eta_k^\nu\right|_p \geq \left|\sum_{k=0}^{n} b_k\right|_p$$

Let Q be the unique polynomial of degree at most n such that

$$Q(z) \equiv z^{-m-1} (\mathrm{mod}\ \eta_0, \dots, \eta_n).$$

Thus (by Theorem 3) we have Newton's formula for $Q(z)$

$$Q(z) = \sum_{k=0}^{n} [\eta_0, \dots, \eta_k; z^{-m-1}](z-\eta_0)\dots(z-\eta_{k-1}).$$

$$= \sum_{k=0}^{n} q_k z^k ,$$

say. Now, by Example 7.2.3, we see that

$$[\eta_0, \dots, \eta_r; z^{-m-1}] = |(\eta_0\eta_1\dots\eta_r)^{-1}[\eta_0^{-1}, \eta_1^{-1}, \dots, \eta_r^{-1}; z^{m+r}]|_p \quad (0 \leqslant r \leqslant n).$$

And, by Example 7.2.1, since $|\eta_i^{-1}|_p \leqslant 1$ for all i,

$$|[\eta_0^{-1}, \dots, \eta_r^{-1}; z^{m+r}]|_p \leqslant 1 .$$

Hence

$$|[\eta_0, \dots, \eta_r; z^{-m-1}]|_p \leqslant |\eta_0\eta_1\dots\eta_r|_p^{-1} \quad (0 \leqslant r \leqslant n),$$

and using Newton's formula above and the fact that $|\eta_i|_p^{-1} \leqslant 1$ for all i, we see that

$$|q_k|_p \leqslant 1 \quad (0 \leqslant k \leqslant n).$$

By the equation (8.2),

$$|\sum_{k=0}^{n} b_k \eta_k^{-m-1}|_p \leqslant \left(\max_{0 \leqslant i \leqslant n} |\sum_{k=0}^{n} b_k \eta_k^{i}|_p\right).$$

Writing $b_k \eta_k^{m+1}$ for b_k, we get the required result.

<u>Theorem 8.3</u> (p-adic analogue of Turan's second main theorem). Let $\rho \in \Omega_p \sim \{0\}$. Let $b_0, \dots, b_n$ and $\eta_0, \dots, \eta_n$ be two sequences of numbers in Ω_p such that

$$0 = |\eta_0|_p \leqslant |\eta_1|_p \leqslant \dots \leqslant |\eta_n|_p < |\rho|_p .$$

Let also f be an analytic function in $|z|_p \leqslant |\rho|_p$. Put

$$M(|r|_p) = \max\{|f(z)|_p ; \ |z|_p = |r|_p\} .$$

Then

$$\left|\sum_{k=0}^{n} b_k f(\eta_k)\right|_p \leqslant \begin{cases} M(|\rho|_p) \max_{0\leqslant i\leqslant n} \left|\sum_{k=0}^{n} b_k \eta_k^i\right|_p & (|\rho|_p \geqslant 1) \\ |\rho|_p^{-n}\ M(|\rho|_p) \max_{0\leqslant i\leqslant n} \left|\sum_{k=0}^{n} b_k \eta_k^i\right|_p & (|\rho|_p < 1)\ . \end{cases}$$

<u>Proof.</u> Let $Q(z) = \sum_{k=0}^{n} q_k z^k$ be the unique polynomial of degree at most n satisfying

$$Q \equiv f \pmod{\eta_0,\dots,\eta_n}.$$

Then (by Theorem 7.3) we have Newton's formula

$$Q(z) = \sum_{k=0}^{n} [\eta_0,\dots,\eta_k;f](z-\eta_0)\dots(z-\eta_{k-1}).$$

It follows easily from either of the expressions for $[\eta_0,\dots,\eta_k;f]$ that

$$|[\eta_0,\dots,\eta_k;f]|_p \leqslant |\rho|_p^{-k} M(|\rho|_p) \qquad (0\leqslant k\leqslant n),$$

and it then follows from both expressions of Q that for $0\leqslant k\leqslant n$,

$$|q_k|_p \leqslant \begin{cases} M(|\rho|_p) & (|\rho|_p \geqslant 1) \\ |\rho|_p^{-k} M(|\rho|_p) & (|\rho|_p < 1)\ . \end{cases}$$

By (8.2) of Lemma 8.1, we obtain the desired result.

3. <u>Basic results on p-adic exponential polynomials.</u>

Throughout this and the next section, the following notation will be used. Let θ be a fixed positive real number; $\omega_1,\dots,\omega_m$ be a sequence of distinct numbers in Ω_p such that

$$|\omega_i|_p \leqslant p^{-\frac{1}{(p-1)} - \theta}\ . \tag{8.3}$$

Put

$$W = \max\{|\omega_i|_p;\ i = 1,2,\dots,m\}\ . \tag{8.4}$$

We consider a fixed exponential polynomial

(8.5) $$E(z) = \sum_{k=1}^{m} \sum_{s=0}^{\rho(k)} a_{ks} z^{s-1} e^{\omega_k z} \qquad (|z|_p < p^{\theta}),$$

where $a_{ks} \in \Omega_p$ $(k=1,\ldots,m;\ s=0,\ldots,\rho(k))$. The a_{ks} will be referred to as the coefficients of E. From Proposition 6.19, it is evident that E is analytic in $|z|_p < p^{\theta}$. For brevity, we write

(8.6) $$M(R) = \max\{|E(z)|_p;\ |z|_p = R\}.$$

Define the sequence

$$(\eta_0, \eta_1, \ldots, \eta_{n-1}) = (\omega_1, \ldots, \omega_1, \omega_2, \ldots, \omega_2, \ldots, \omega_m, \ldots, \omega_m)$$

where ω_k is repeated $\rho(k)$ times $(1 \leq k \leq m)$ and $\sum_{k=1}^{m} \rho(k) = n$. Now let v be a fixed number in Ω_p such that

(8.7) $$|v|_p < p^{\theta}.$$

Define an analytic function

$$f(z) = \exp(vz) \qquad (|z|_p \leq p^{-\frac{1}{(p-1)} - \theta}).$$

The main aim is to obtain a bound for $M(\gamma R)/M(R)$, for some real $\gamma \geq 1$, by estimating the coefficients of the unique polynomial Q of degree at most $n-1$ satisfying

(8.8) $$Q \equiv f \pmod{\eta_0, \ldots, \eta_{n-1}}.$$

We write

$$[\eta_0, \ldots, \eta_r] = [\eta_0, \ldots, \eta_r; f] \qquad (0 \leq r \leq n-1).$$

The following lemmas establish the relationship between E and Q and bounds of the coefficients of Q.

Lemma 8.4. Let E, v, Q be defined as (8.5), (8.7), (8.8) and let

(8.9) $$Q(z) = \sum_{\ell=0}^{n-1} q_{\ell} z^{\ell}.$$

Then

(8.10) $$E(v) = \sum_{\ell=0}^{n-1} q_\ell E^{(\ell)}(0)$$

Proof. Since, by Theorems 7.2 and 7.3,

$$e^{vz} = Q(z) + [z,\eta_0,\ldots,\eta_{n-1}](z-\eta_0)\ldots(z-\eta_{n-1}),$$

then

$$Q^{(s-1)}(\omega_k) = \left(D^{s-1}e^{vz}\right)_{z=\omega_k} = v^{s-1}e^{\omega_k v}$$

$$\left(1 \leqslant k \leqslant m,\ 0 \leqslant s \leqslant \rho(k)\right) .$$

Therefore

$$E(v) = \sum_{k=1}^{m} \sum_{s=0}^{\rho(k)} a_{ks}Q^{(s-1)}(\omega_k) .$$

Also, from (8.9) we have

$$Q^{(s-1)}(\omega_k) = \sum_{\ell=0}^{n-1} q_\ell \binom{\ell}{s-1}(s-1)!\ \omega_k^{\ell-s-1} .$$

Substituting for $Q^{(s-1)}(\omega_k)$ in the equation for $E(v)$, we get

$$E(v) = \sum_{\ell=0}^{n-1} q_\ell \Big(\sum_{k=1}^{m} \sum_{s=0}^{\rho(k)} a_{ks}\binom{\ell}{s-1}(s-1)!\ \omega_k^{\ell-s+1}\Big) .$$

But by differentiating $E(z)$ in (8.5) and putting $z=0$, we get

$$E^{(\ell)}(0) = \sum_{k=1}^{m} \sum_{s=0}^{\rho(k)} a_{ks}\binom{\ell}{s-1}(s-1)!\ \omega_k^{\ell-s+1} .$$

Hence

$$E(v) = \sum_{\ell=0}^{n-1} q_\ell E^{(\ell)}(0).$$

Lemma 8.5. Let E, Q and $q_0,\ldots,q_{n-1}$ be as in Lemma 8.4 and W as in (8.4). Then

(8.11) $$|q_k|_p \leqslant \max\left\{\left|\frac{v^k}{k!}\right|_p,\ \max_{r\geqslant n}\left|\frac{v^r}{r!}\right|_p W^{r-k}\right\} \qquad (0 \leqslant k \leqslant n-1)$$

(8.12) $$\leqslant \max\left\{\left|\frac{v^k}{k!}\right|,\ \max_{r\geqslant k+1}\left|\frac{v^r}{r!}\right|_p W^{r-k}\right\} .$$

Proof. Since

$$Q(z) \equiv \exp(vz) \pmod{\eta_0,\ldots,\eta_{n-1}},$$

the result follows from Theorem 7.11, keeping in mind that in this case $|c_{rk}|_p \leqslant W^{r-k}$.

Next we apply both lemmas to obtain an estimate of the size of E. It appears that both (8.11) and (8.12) give bounds of similar size so only (8.12) will be used.

Theorem 8.6. Let W, E, M be defined as in (8.4), (8.5) and (8.6). Let v be as in (8.7) and $u \in \Omega_p$ be such that

$$|u|_p \leqslant |v|_p.$$

Then

(8.13)

$$M(|v|_p) \leqslant M(|u|_p) \max_{0\leqslant k\leqslant n-1} \max\left\{\left|\frac{v}{u}\right|_p^k, \max_{r\geqslant k+1}\left|\frac{v^r}{r!}\right|_p W^{r-k}\left|\frac{k!}{u^k}\right|_p\right\}.$$

Proof. From (8.10), we get

$$M(|v|_p) \leqslant \max_{0\leqslant k\leqslant n-1} |q_k E^{(k)}(0)|_p .$$

Now by Proposition 6.15 (p-adic Cauchy's inequality)

$$|E^{(k)}(0)|_p \leqslant |k!u^{-k}|_p \; M(|u|_p) \qquad (k \in Z^+).$$

Thus

$$M(|v|_p) \leqslant M(|u|_p) \max_{0\leqslant k\leqslant n-1} |q_k k! u^{-k}|_p .$$

Using Lemma 8.5, we obtain

$$M(|v|_p) \leqslant M(|u|_p) \max_{0\leqslant k\leqslant n-1} \max\left\{\left|\frac{v}{u}\right|_p^k, \max_{r\geqslant k+1}\left|\frac{v^r}{r!}\right|_p W^{r-k}\left|\frac{k!}{u^k}\right|_p\right\}.$$

Corollary 8.7. Let W, E, M be as in Theorem 8.6. For any positive integer

$$k = a_0 + a_1 p + \ldots + a_t p^t ,$$

where $a_i \in \{0,1,\ldots,p-1\}$ $(i = 0,\ldots,t)$ and $a_t \neq 0$, we write

$$s(k) = a_0 + a_1 + \dots + a_t \,.$$

Let θ be as before and ε be a positive real number such that

$$0 < \varepsilon < \tfrac{1}{2}\theta \,.$$

Then

(8.14) $$M(p^{\theta-\varepsilon}) \leqslant M(p^{\varepsilon})\; p^{(\theta-2\varepsilon)(n-1)} \max\{1, p^{-\varepsilon+(s-1)/(p-1)}\} \,,$$

where $s = \max\limits_{0\leqslant k\leqslant n-1} s(k)$, and

(8.15) $$M(p^{\theta-\varepsilon}) \leqslant M(p^{\varepsilon})\; p^{(\theta-2\varepsilon)(n-1)} \max\{1, p^{-\varepsilon+[\log_p(n-1)]+1-1/(p-1)}$$

Proof. If in Theorem 8.6 we put

$$|u|_p = p^{\varepsilon}, \quad |v|_p = p^{\theta-\varepsilon}, \quad W = p^{-1/(p-1)-\theta},$$

then we get

$$\max_{0\leqslant k\leqslant n-1} \left|\frac{v^k}{u}\right|_p = p^{(\theta-2\varepsilon)(n-1)},$$

and using Proposition 6.20, for $0 \leqslant k \leqslant n-1$, $r \geqslant k+1$, we have

$$\left(\left|\frac{v^r}{r!}\right|_p W^r\right)\left(\left|\frac{k!}{u^k}\right|_p W^{-k}\right) = p^{-\varepsilon r - \frac{s(r)}{p-1}} \cdot p^{(\theta-\varepsilon)k + \frac{s(k)}{p-1}}$$

$$\leqslant p^{-\varepsilon(k+1)+(\theta-\varepsilon)k+\frac{s(k)-1}{p-1}}$$

(using $s(r) \geqslant 1$)

$$\leqslant p^{(\theta-2\varepsilon)(n-1)-\varepsilon+\frac{s-1}{p-1}}$$

Hence by Theorem 8.6, we get

$$M(p^{\theta-\varepsilon}) \leqslant M(p^{\varepsilon})\; p^{(\theta-2\varepsilon)(n-1)} \max\left\{1, p^{\frac{s-1}{p-1}-\varepsilon}\right\} .$$

To obtain (8.15) we note that if

$$k = a_0 + a_1 p + \dots + a_t p^t \,,$$

then

$$s(k) = a_0 + \dots + a_t \leqslant (p-1)(t+1) \leqslant (p-1)([\log_p k]+1) .$$

Replacing s by $(p-1)([\log_p(n-1)]+1)$ in (8.14) we obtain (8.15).

Now we are in a position to estimate the number of zeros of E in the p-adic case similar to Theorem 6.1 of Chapter 6.

Theorem 8.8. If E is as defined in (8.5) and is not identically zero, then the number of zeros of E in $|z|_p \leqslant 1$ does not exceed

$$(n-1) + \max\{0, [\log_p(n-1)]+1-1/(p-1)\}/\theta,$$

provided $n > 1$.

Proof. Let $\alpha_1, \ldots, \alpha_h$ be all zeros of E in $|z|_p \leqslant 1$ taken with multiplicities. (The number is finite by the Corollary to Theorem 7.8.) Define

$$G(z) = (z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_h).$$

Clearly, E/G is an analytic function in $|z|_p < p^\theta$. Therefore, by the maximum-modulus theorem (Proposition 6.14) we have

$$\frac{M(p^{\theta-\varepsilon})}{p^{(\theta-\varepsilon)h}} \geqslant \frac{M(p^\varepsilon)}{p^{\varepsilon h}}$$

where θ, ε are as before $(\varepsilon < \frac{1}{2}\theta)$. Thus

$$p^{(\theta-2\varepsilon)h} \leqslant M(p^{\theta-\varepsilon})/M(p^\varepsilon)$$

Using the estimate (8.15) we get

$$h \leqslant (n-1) + \max\{0, -\varepsilon+[\log_p(n-1)]+1-1/(p-1)\}/(\theta-2\varepsilon).$$

For each fixed θ, ε is arbitrary with $0 < \varepsilon < \frac{1}{2}\theta$; by letting $\varepsilon \to 0$, the required result follows.

The bound obtained in Theorem 8.8 for h is better than that obtained by Shorey [38] and is similar to that in van der Poorten [33]. In fact, in Shorey [38]

$$h \leqslant \frac{90}{\theta \log p} + \frac{30}{\theta}\left(\frac{1}{p-1} + \theta\right)(n-1)$$

and in van der Poorten [33]

$$h < (n-1) + \max_{0 \leqslant r < p-1} \{[\log_p(n+r)] - r/(p-1)\}/\theta .$$

→ p141.

If $n<p$, it is better to use (8.14) with $s=n$ to get the bound

$$h \leqslant n-1+(n-1)/(p-1)\theta$$

which is that obtained in van der Poorten [32].

4. The estimate on bound of p-adic exponential polynomials.

In this section a bound for the size of coefficients of a p-adic exponential polynomial will be obtained similar to Theorem 6.7. ?? new? required??

Theorem 8.9. Let θ be a fixed positive real number; $\omega_1,\ldots,\omega_m \in \Omega_p$ be such that

$$|\omega_i|_p \leqslant p^{-1/(p-1)-\theta} \qquad (i=1,\ldots,m);$$

$\rho(1),\ldots,\rho(m)$ and n be non-negative integers with

$$n=\sum_{k=1}^{m}\rho(k) \;;$$

$r_1,\ldots,r_\ell$ and r be non-negative integers with

$$r=\sum_{i=1}^{\ell} r_i \;;$$

$\beta_1,\ldots,\beta_\ell \in \Omega_p$ be distinct such that

$$|\beta_i|_p \leqslant 1 \qquad (i=1,\ldots,\ell);$$

$E(z)$ be an exponential polynomial of the form (8.5). For fixed integers M, N such that

$$1\leqslant M\leqslant m, \quad 0\leqslant N\leqslant \rho(M)-1,$$

let w_1, w_2, b_1, b_2, E be positive real numbers such that,

$$\prod_{\substack{i=1\\ i\neq M}}^{m} |\omega_M-\omega_i|_p^{\rho(i)} \geqslant w_1\,, \quad |\omega_M-\omega_i|_p^{\rho(M)} \geqslant w_2 \qquad (1\leqslant i\leqslant m,\ i\neq M)$$

$$\prod_{i=1}^{\ell} |\beta_j-\beta_i|_p^{r_i} \geqslant b_1 \qquad (i\neq j,\ 1\leqslant j\leqslant \ell),$$

$$|\beta_j-\beta_i|_p^{r_i} \geqslant b_2 \qquad (i\neq j,\ 1\leqslant i\leqslant \ell,\ 1\leqslant j\leqslant \ell),$$

$$|E^{(i)}(\beta_j)/i!|_p \leqslant E \qquad (0\leqslant i\leqslant r_j-1,\ 1\leqslant j\leqslant \ell).$$

If

(8.16) $\quad r > (n-1) + \max\{0,[\log_p(n-1)] + 1 - 1/(p-1)\}/\theta$,

then

$$|N!a_{MN}|_p < (b_1b_2w_1w_2)^{-1}w_2^{(N+1)/\rho(M)}\ E\ ,$$

where a_{MN} is the coefficient of $z^{N-1}\exp(\omega_M z)$ in $E(z)$.

Before proving this theorem, a few auxiliary results are required.

Lemma 8.10. Let M,N be as above, and let $Q_{MN}(z)$ be the unique polynomial $\sum_{i=0}^{n-1} q_i z^i$ satisfying

$$Q_{MN}^{(\mu)}(\omega_\nu) = \begin{cases} 1 & (\mu = N,\quad \nu = M) \\ 0 & (\mu \neq N,\quad \nu \neq M,\ 1 \leqslant \nu \leqslant m,\\ & \qquad 0 \leqslant \mu \leqslant \rho(\nu)-1). \end{cases}$$

Then

$$a_{MN} = \sum_{i=0}^{n-1} q_i E^{(i)}(0)$$

Proof. As in the proof of Lemma 8.4,

$$E^{(i)}(0) = \sum_{\nu=1}^{m}\sum_{\mu=0}^{\rho(\nu)} a_{\nu\mu}\binom{i}{\mu-1}(\mu-1)!\,\omega_\nu^{i-\mu+1}$$

$$= \left[\sum_{\nu=1}^{m}\sum_{\mu=0}^{\rho(\nu)} a_{\nu\mu}D^{\mu-1}z^i\right]_{z\,=\,\omega_\nu}.$$

Thus

$$\sum_{i=0}^{n-1} q_i E^{(i)}(0) = \left[\sum_{\nu=1}^{m}\sum_{\mu=0}^{\rho(\nu)} a_{\nu\mu}\sum_{i=0}^{n-1} q_i D^{\mu-1}z^i\right]_{z\,=\,\omega_\nu}$$

$$= \sum_{\nu=1}^{m}\sum_{\mu=0}^{\rho(\nu)} a_{\nu\mu}Q_{MN}^{(\mu)}(\omega_\nu) = a_{MN}\ .$$

Lemma 8.11. Let Q_{MN} be as in Lemma 8.10. Then

$$|N!q_i|_p \leqslant (w_1w_2)^{-1}w_2^{(N+1)/\rho(M)}\ .$$

Proof. We first note that by Proposition 6.14(i) we have

$$|q_i|_p \leqslant \max\{|Q_{MN}(z)|;\ |z|_p = 1\}\ .$$

Hence it is sufficient to prove that if $|z|_p = 1$, then

$$|N!Q_{MN}(z)|_p \leqslant (w_1 w_2)^{-1} w_2^{(N+1)/\rho(M)} .$$

Let $\varepsilon \in R$ be such that $0 < \varepsilon < w_2^{1/\rho(M)}$. Taking $|\rho|_p = w_2^{1/\rho(M)} - \varepsilon$, $|z|_p = 1$ in Theorem 7.12 and note that

$$\max\{|\rho^{\rho(M)}(\varphi(u))^{-1}|_p;\ |u-\omega_M| = |\rho|_p\} \leqslant w_1^{-1} ,$$

we hence obtain

$$|N!Q_{MN}(z)|_p \leqslant (w_2^{1/\rho(M)}-\varepsilon)^{(N+1-\rho(M))} w_1^{-1} .$$

This inequality holds for any ε such that $0 < \varepsilon < w_2^{1/\rho(M)}$, and on letting $\varepsilon \to 0$, we get the required result

Lemma 8.12. Let $\beta_1,\ldots,\beta_\ell$, E,b be as defined in Theorem 8.9; let $P(z)$ be the unique polynomial of degree at most $r-1$ such that

$$E^{(i)}(\beta_j) = P^{(i)}(\beta_j) \qquad (1 \leqslant j \leqslant \ell;\ 0 \leqslant i \leqslant r_j - 1).$$

Let $\varepsilon \in R$ be such that $0 < \varepsilon < \frac{1}{2}\theta$. If $v \in \Omega_p$ be such that $|v|_p = p^\varepsilon$, then

$$|P(v)|_p < p^{(r-1)\varepsilon}(b_1 b_2)^{-1} E .$$

Proof. The idea of proof is the same as that in Lemma 8.11, that is of applying the method of proof of Theorem 7.12 to the expression for $P(z)$ obtained from Theorem 7.7.

Proof of Theorem 8.9. For any ε such that $0 < \varepsilon < \frac{1}{2}\theta$, we have by Property 6.15 (Cauchy's inequality)

(8.17) $$|E^{(i)}(0)|_p \leqslant |i!|_p\, p^{-\varepsilon i} M(p^\varepsilon) \leqslant M(p^\varepsilon) \qquad (i = 0,\ldots,n-1),$$

where $M(p^\varepsilon) = \max\{|E(z)|_p;\ |z|_p = p^\varepsilon\}$.

Note that from (8.16) we have for all sufficiently small $\varepsilon > 0$, (8.18) $\quad r \geqslant (n-1) + \max\{0, [\log_p(n-1)]+1-1/(p-1)\}/(\theta-2\varepsilon)$.

Consider a fixed $\varepsilon > 0$ such that (8.18) holds, and fix $\rho \in \Omega_p$ such that $|\rho|_p = p^{\theta-\varepsilon}$. Let P be the polynomial defined in Lemma 8.12. By applying Theorem 7.7 to $E(z)$, for $|z|_p < |\rho|_p$ we have

$$E(z) - P(z) = \int_{0,\rho} \frac{\psi(z)E(u)\,udu}{(u-z)\psi(u)}$$

where $\psi(z) = (z-\beta_1)^{r_1}\ldots(z-\beta_\ell)^{r_\ell}$. Therefore, by Proposition 6.11

$$|E(z)-P(z)|_p \leqslant |\psi(z)|_p\, p^{(\varepsilon-\theta)r} M(p^{\theta-\varepsilon}) .$$

Now choose the point $z = v$ such that

$$|v|_p = p^{\varepsilon} , \qquad |E(v)|_p = M(p^{\varepsilon}) .$$

Thus

$$|E(v)-P(v)|_p \leqslant p^{(2\varepsilon-\theta)r} M(p^{\theta-\varepsilon}) < M(p^{\varepsilon}) ,$$

using (8.5) of Corollary 8.7 and (8.18).

Thus by the strong triangle inequality and (8.17)

$$|P(v)|_p = |P(v)-E(v)+E(v)|_p = |E(v)|_p = M(p^{\varepsilon}) \geqslant |E^{(i)}(0)|_p$$
$$(i = 0,\ldots,n-1) ,$$

From Lemmas 8.10, 8.11, 8.12 and this last inequality, we get

$$|N!a_{MN}|_p \leqslant \max_{i=0,\ldots,n-1} |N!q_i E^{(i)}(0)|_p$$
$$\leqslant (w_1w_2)^{-1} w_2^{(N+1)/\rho(M)} |P(v)|_p$$
$$\leqslant (b_1b_2w_1w_2)^{-1} p^{(r-1)\varepsilon}\, E\, w_2^{(N+1)/\rho(M)} .$$

Since this holds for all sufficiently small ε satisfying (8.18).

Continued :

As can be readily checked the bound on $N!a_{MN}$ obtained in Theorem 8.9 above implies that stated in the introduction (page 13) of van der Poorten [33]. However, our method of proof is simpler and it seems to be a more natural approach to problems related to interpolation.

BIBLIOGRAPHY

[1] ADAMS, W.W., "Transcendental numbers in the p-adic domain", Amer. J. Math. 88 (1966), 279-308.

[2] ADAMS, W.W. and STRAUS, E.G., "Non-archimedean analytic functions taking the same values at the same points", Illinois J. Math. 15 (1971), 418-424.

[3] AHLSWEDE, R. and BOJANIC, R., "Approximation of continuous functions in p-adic analysis", J. Approximation Theory 15 (1975), 190-205.

[4] AMICE, Y., "Interpolation p-adique", Bull. Soc. Math. France 92 (1964), 117-180.

[5] BACHMAN, G., "Introduction to p-adic numbers and valuation theory", Academic Press, New York, 1964.

[6] BAKER, A., "Transcendental number theory", Cambridge University Press, Cambridge, 1975.

[7] BALKEMA, A.A. and TIJDEMAN, R., "Some estimates in the theory of exponential sums", Acta Math. Acad. Sci. Hungary 24 (1973), 115-133.

[8] BILLINGSLEY, P., "Ergodic theory and information", John Wiley and Sons, New York, 1965.

[9] CASSELS, J.W.S., "An introduction to diophantine approximation", Cambridge Tract in Mathematics and Mathematical Physics number 45, Cambridge, 1965.

[10] CHENEY, E.W., "Introduction to approximation theory", McGraw Hill, New York, 1966.

[11] CHERNOFF, P.R., RASALA, R.A. and WATERHOUSE, W.C., "The Stone-Weierstrass theorem for valuable fields", Pacific J. Math. (2), 7 (1968), 233-240.

[12] DIEUDONNÉ, J., "Sur les fonctions continues p-adiques", Bull. Sci. Math. (2), 68 (1944), 74-95.

[13] GALAMBOS, J., "The distribution of the largest coefficient in continued fraction expansion", Quart. J. Math. Oxford (2), 23 (1972), 147-151.

[14] GELFOND, A.O., "Calculus of finite differences", Hindustan Publishing Cooperation, Delhi, 1971.

[15] GELFOND, A.O., "Transcendental and algebraic numbers", Dover Publications, New York, 1960.

[16] HARDY, G.H. and WRIGHT, E.M., "An introduction to the theory of numbers", Oxford University Press, Oxford, 1971.

[17] KHINTCHINE, A., "Continued fractions", The University of Chicago Press, Chicago, 1964.

[18] KOKSMA, J.F., "Diophantische Approximationen", Ergebnisse d. Math. u. ihrer Grenzgebiete 4,4., Berlin und Leipzig, 1936.

[19] LUTZ, E., "Sur les approximations diophantiennes lineáres p-adiques", Actualités Scientifiques et Industrielles, 1224, Paris, 1955.

[20] MAHLER, K., " Über Diophantische Approximationen im Gebiete der p-adischen Zahlen", Jahresb. Deutschen Math. Verein. 44 (1934), 250-255.

[21] ________, "Zur Approximation p-adischer Irrationalzahlen", Nieuw Arch. Wisk. 18 (1934), 22-34.

[22] ________, "Ein p-adisches Analogen zu einem Satz von Tchebycheff", Mathematica, Zutphen. 7 (1938), 2-6.

[23] ________ , "On a geometrical representation of p-adic numbers", Ann. of Math. 41 (1940), 8-56.

[24] ________ , "An interpolation series for continuous functions of a p-adic variable", J. Reine Angew. Math. 199 (1958), 24-34; with a correction in J. Reine Angew. Math. 208 (1961), 70-72.

[25] ________ , "Lectures on diophantine approximations; Part 1: g-adic numbers and Roth's theorem", University of Notre Dame Press, 1961.

[26] ________ , "Introduction to p-adic numbers and their functions", Cambridge University Press, Cambridge, 1973.

[27] MÁRKI, I. and SZABADOS, J., "Interpolation and best polynomial approximation in the domain of p-adic integers", Analysis Math. 2 (1976), 277-285.

[28] MONNA, A.F., "Remarks on some problems in linear topological spaces over fields with non-archimedean valuation", Proc. Kon. Ned. Akad. Wetensch. 71 (1968), 484-496.

[29] ________ , "Analyse non-archimédienne", Springer-Verlag, Berlin, 1970.

[30] NARICI, L., BECKENSTEIN, E., and BACHMAN, G., "Functional analysis and valuation theory", Marcel Dekker, New York, 1971.

[31] PERRON, O., "Die Lehre von den Kettenbrüchen; Band I, II", Teubner, Stuttgart, 1954.

[32] van der POORTEN, A.J., "Zeros of p-adic exponential polynomials", Proc. Kon. Ned. Akad. Wetensch. 79 (1976), 46-49.

[33] ____________________, "Hermite interpolation and p-adic exponential polynomials", J. Aust. Math. Soc. 22 (1976), 12-26.

[34] RUBAN, A.A., "Certain metric properties of the p-adic numbers", Sibirsk. Mat. Ž. 11 (1970), 222-227. English translation: Siberian Math. J. 11 (1970), 176-180. [Trans. not consulted.]

[35] __________, "The Perron algorithm for p-adic numbers and some of its ergodic properties", Soviet Math. Dokl. (trans.) (3), 13 (1972), 606-609.

[36] __________, "An invariant measure for a transformation related to Perron's algorithm for p-adic numbers", Soviet Math. Dokl. (trans.) (6), 14 (1973), 1752-1754.

[37] SCHNEIDER, Th., "Über p-adische Kettenbrüche", Symposia Math. 4 (1970), 181-189.

[38] SHOREY, T.N., "Algebraic independence of certain numbers in the p-adic domain", Proc. Kon. Ned. Akad. Wetensch. 75 (1972), 423-435.

[39] __________, "P-adic analogue of a theorem of Tijdeman and its application", Proc. Kon. Ned. Akad. Wetensch. 75 (1972), 436-442.

[40] TAYLOR, S.J., "Introduction to measure and integration", Cambridge University Press, Cambridge, 1973.

[41] TURAN, P., "Ein neue Methode in der Analysis und deren Anwendungen", Budapest, 1953.

[42] TURKSTRA, H., "Metrische bijdragen tot de theorie Diophantische approximaties in het lichaam der p-adische getallen", Thèse, Gröningen, 1936.

[43] WALSH, J.L., "Interpolation and approximation by rational functions in the complex domain", American Math. Soc. Colloq. Publications vol. 20, New York, 1935.