

P-ADIC NUMBERS

By

RICHARD PRESTON SAVAGE

Bachelor of Science  
University of Chattanooga  
Chattanooga, Tennessee  
1955


Master of Science  
Oklahoma State University  
Stillwater, Oklahoma  
1957

Submitted to the Faculty of the  
Graduate College of the  
Oklahoma State University  
in partial fulfillment of  
the requirements for  
the Degree of  
DOCTOR OF EDUCATION  
May, 1968

OCT 27 1968


P-ADIC NUMBERS

Thesis Approved:

  
Thesis Adviser

  
\_\_\_\_\_

  
\_\_\_\_\_

  
\_\_\_\_\_

  
Dean of the Graduate College

688734

## PREFACE

The serious student of mathematics generally studies a systematic development of the real number system either as an advanced undergraduate or beginning graduate student. The usual approach is to develop the natural numbers from the Peano axioms, the integers as equivalence classes of ordered pairs of natural numbers, the rational numbers as equivalence classes of ordered pairs of integers, and the real numbers as equivalence classes of Cauchy sequences of rational numbers.

The primary purpose of this study is to develop another type of number system, the p-adic numbers, from the rational numbers in a manner quite similar to that used in developing the reals from the rationals. A few of the more important properties of the p-adic numbers are then investigated.

It is believed that Theorem 8 of Chapter II may constitute an addition to the previously known results concerning solutions of the congruence  $x^n \equiv a \pmod{m}$ . It is possible, also, that the proof of Theorem 8 of Chapter III concerning the representation of a p-adic number as a

power series may be original with this study.

There are many who have helped directly or indirectly with this study, and I wish to express my appreciation to them. I am deeply indebted to my committee members, Drs. H. S. Mendenhall, Milton E. Berg, Gerald K. Goff, Vernon Troxel, and Norman E. Wilson for their advice and assistance in this study and in planning the prerequisite academic program. Particularly, I wish to thank Dr. Goff who as thesis adviser followed this study from its inception and made many helpful suggestions. Special thanks are due also to Miss Mattie Sue Cooper, Reference Librarian at Tennessee Technological University, for her help in securing reference material, to Orion Miller who typed the original manuscript, and to Mrs. Catherine Owens who typed the final version. Finally, I wish to express my very deep appreciation to my wife, Anna, and to my sons, Richard, Jr., Robert, Michael, and Stephen. Neither this study nor the work leading to it would have been possible without their help and understanding.

## TABLE OF CONTENTS

Chapter	Page
I. INTRODUCTION. . . . .	1
Organization of the Study . . . . .	1
Need for Study. . . . .	3
II. MODULAR ARITHMETIC . . . . .	4
M-adic Numbers. . . . .	17
III. VALUATIONS . . . . .	23
Metrics . . . . .	30
P-adic Numbers. . . . .	31
IV. THE P-ADIC FIELDS. . . . .	46
Summary and Conclusions . . . . .	54
BIBLIOGRAPHY. . . . .	56

## CHAPTER I

### INTRODUCTION

The  $p$ -adic numbers were discovered by Kurt Hensel (5) near the end of the last century. Seventy years later, however, the average mathematician has probably never heard of them. This undoubtedly can be attributed largely to the fact that they have been mentioned so infrequently in mathematical literature. While it is true that their primary importance has been in the fields of algebraic number theory and algebraic geometry, it is felt by this writer that there is adequate justification for their study by mathematicians in other fields as well. This investigation was prompted by this belief, and it makes an effort to present the basic theory of  $p$ -adic numbers to a wide mathematical audience. As far as most of the study is concerned, however, the prerequisite mathematical preparation of the reader would have to be comparable to that of the advanced undergraduate or beginning graduate student.

#### Organization of Study

Most of Chapter II is devoted to a consideration of the

arithmetic of congruence classes modulo  $m$  with considerable emphasis being placed on the case where  $m$  is a prime number. Through this study of modular arithmetic, some of the basic results of elementary number theory are established in a very simple manner. A consideration of division modulo  $m$  paves the way for the introduction of Hensel's  $p$ -adic numbers, albeit in a manner much different from that employed by Hensel. Much of Chapter II could be understood by the high school senior or the college freshman who is reasonably proficient in mathematics, and it is hoped that an investigation of this chapter might help arouse in him the spirit of discovery.

Chapter III constitutes the main body of the study. It is concerned first with a detailed discussion of valuation theory. The  $p$ -adic numbers are then introduced as a completion of the rational field with respect to a  $p$ -adic metric derived from the  $p$ -adic valuation of the rational field. The close parallel which exists between the  $p$ -adic completion of the field of rational numbers and the real completion of the same field is carefully emphasized. Finally, it is established that there are only two basic types of completions of the rational field.

Chapter IV concludes the study with an investigation of a few of the most important properties of  $p$ -adic numbers.

It establishes that the p-adic fields are not isomorphic to the field of real numbers, but it does point out some interesting points of similarity between the p-adic fields and the real field. Finally, Chapter IV suggests directions for further reading and research.

#### Need for Study

Today's mathematics student studies a systematic development of the real number system either as an advanced undergraduate or as a beginning graduate student. In the course of this development he encounters the field of real numbers as a completion of the field of rational numbers. Since there is only one other possible type of completion of the rational field, a p-adic completion, it seems to the writer that it should receive at least passing attention during any such study. The literature regarding the development of the p-adic numbers is, however, quite limited. It is hoped that this study may help alleviate this situation by collecting in one volume the essentials for understanding p-adic numbers.



## CHAPTER II

### MODULAR ARITHMETIC

Early in life the child is introduced to modular arithmetic in the form of arithmetic on the clock. He learns that on the ordinary clock  $9+4=1$ ,  $6+8=2$ , and so on. In this arithmetic all multiples of 12 are "thrown away" and it is only the remainder in which he is interested, unless the remainder is 0, in which case he adds 12. For this arithmetic a base twelve numeration system would be particularly advantageous since the sum of two numbers on the clock would then be the last digit of the ordinary sum except in the case of 0 as a last digit. If the "12" on the clock were replaced by "0" and base 12 numerals were used, then in all cases the sum of two numbers in the clock arithmetic would be given by the last digit of their ordinary sum.

Since the reader is undoubtedly much more familiar with base ten than with any other base, a few examples in modulo 10 arithmetic should serve to clarify the above ideas.

#### Ordinary Arithmetic

$$3+5=8$$

$$9+6=15$$

$$23+37=60$$

#### Modulo 10 Arithmetic

$$3+5=8$$

$$9+6=5$$

$$23+37=3+7=0$$

Hereafter modulo 10 arithmetic will be called simply 10-arithmetic and "modulo m arithmetic" will be shortened to "m-arithmetic." If m is a prime number, p, then the corresponding modular arithmetic will be referred to as p-arithmetic, and this notation will be used only if p is a prime number.

The complete addition and multiplication tables for 10-arithmetic are as follows:

Addition Table

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Multiplication Table

•	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

It is readily apparent that the sum of two positive integers modulo 10 is just the units digit of their ordinary sum and that the product of two positive integers, modulo 10, is just the units digit of their ordinary product.

Hence if  $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ , and if "+" be the operation defined by the above table then:

$$(1) a \in S, b \in S \implies a+b \in S$$

$$(2) \forall a, b, c \in S, a+(b+c)=(a+b)+c$$

$$(3) \forall a \in S, a+0=a$$

$$(4) \forall a \in S, \exists b \in S \text{ such that } a+b=0$$

$$(5) \forall a, b \in S, a+b=b+a$$

Properties (1), (3), (4), and (5) are immediately apparent from an inspection of the addition table. Property (2), the associative property, is a direct consequence of the corresponding property of ordinary addition. Thus  $S$  forms a commutative or Abelian group with respect to the operation of addition. It is equally apparent that  $S$  does not form a group with respect to multiplication since the identity element for multiplication is 1 and since there exists no element  $a \in S$  such that  $5 \cdot a = 1$ . However, the system  $(S, +, \cdot)$  does inherit the additional properties from ordinary arithmetic that:

$$(6) \forall a, b, c \in S, a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

$$(7) \forall a, b \in S, a \cdot b = b \cdot a$$

$$(8) \forall a, b, c \in S, a \cdot (b+c) = a \cdot b + a \cdot c.$$

Consequently,  $(S, +, \cdot)$  is a commutative ring with unity.

Since only the last digit of a number is of significance in 10-arithmetic, the numbers of 10-arithmetic are defined to be the elements of the set  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . More generally, the numbers of  $m$ -arithmetic are defined to be the elements of the set  $\{0, 1, 2, \dots, (m-1)\}$ .

The addition and multiplication tables for 7-arithmetic

are reproduced below in order to explore the contrast between the multiplication table in 10-arithmetic and the multiplication table of 7-arithmetic.

Addition Table

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplication Table

.	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

An examination of these tables reveals immediately that the set  $T = \{0, 1, 2, 3, 4, 5, 6\}$  forms an Abelian or commutative group with respect to addition, and that the set  $T - \{0\}$  forms a commutative group with respect to multiplication. The distributivity of multiplication over addition is inherited from ordinary arithmetic. Hence the set  $T$  with the two operations of addition and multiplication is a field.

The set  $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  with the operations of addition and multiplication modulo 10 failed to be a field for lack of multiplicative inverses for all non-zero elements of  $S$ . This lack of multiplicative inverses is very closely connected with the fact that  $S$  has zero divisors in 10-arithmetic. For example,  $5 \cdot 2 = 0$ .

The presence of zero divisors in 10 arithmetic

together with their absence in 7-arithmetic suggests the following theorem.

**Theorem 1.** If  $a$  and  $b$  are numbers in  $p$ -arithmetic such that  $a \cdot b = 0$  then  $a = 0$  or  $b = 0$ .

**Proof:**  $a \cdot b = 0$  in  $p$ -arithmetic if and only if there exists an integer  $k$  such that  $a \cdot b = k \cdot p$  in ordinary arithmetic. Since  $p$  is a prime number  $a \cdot b = k \cdot p$  if and only if  $a$  is a multiple of  $p$  or  $b$  is a multiple of  $p$ . Both  $a$  and  $b$  are elements of the set  $\{0, 1, 2, \dots, p-1\}$ , and consequently neither can be a multiple of  $p$  unless it be  $0 \cdot p$ . Thus if  $a \cdot b = 0$  in  $p$ -arithmetic then necessarily  $a = 0$  or  $b = 0$ .

Dynkin and Uspenskii (4) seek to convey graphically an appreciation of the process of multiplication in  $m$ -arithmetic through the use of arrow diagrams. In these diagrams the numbers of  $m$ -arithmetic are represented by points and the result of multiplying  $b$  by  $a$  is indicated by an arrow leading from  $b$  to  $a \cdot b$ . Such multiplication diagrams yield rather readily certain facts which are not immediately apparent from an inspection of the multiplication table.

The diagrams for multiplication by 3 (Figure 1) and by 5 (Figure 2) in 7-arithmetic appear below.

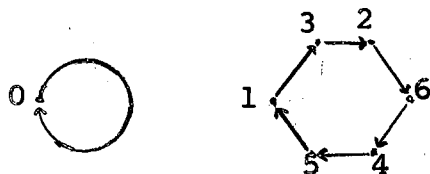


Figure 1

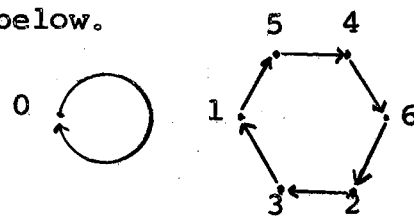
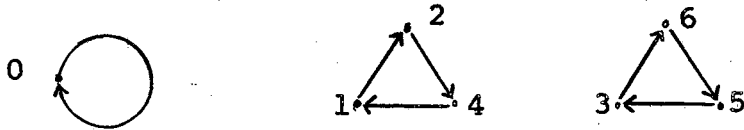
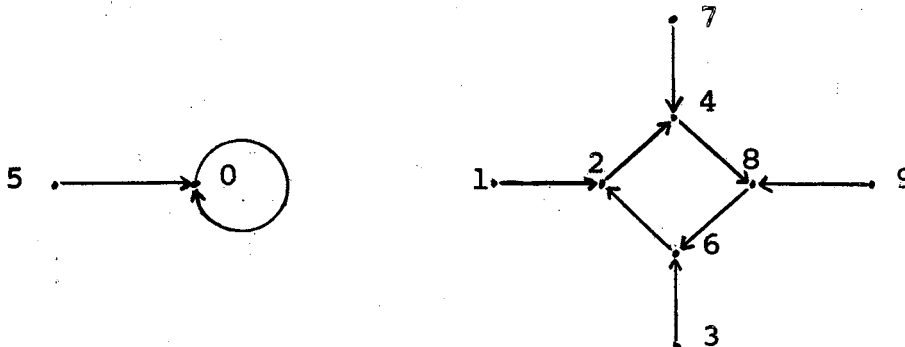


Figure 2

The diagram for multiplication by 2 in 7-arithmetic which is reproduced next has a somewhat different appearance.



In spite of the apparent differences in the above diagrams, it is important to note that every number is at the tip of exactly one arrow and at the tail of exactly one arrow. This phenomenon is described by saying that the diagrams consist of cycles where a cycle is defined to be a sequence of numbers  $\{X_n\}_{n=1}^k$  connected by arrows from  $X_n$  to  $X_{n+1}$ , ( $n=1, \dots, k-1$ ), with a final arrow leading from  $X_k$  to  $X_1$ . If  $k=1$  there is just one arrow which leads from  $X_1$  to itself. Not all multiplication diagrams in  $m$ -arithmetic consist of cycles as evidenced by the following diagram depicting multiplication by 2 in 10-arithmetic.



The diagrams which have been constructed above suggest that in  $m$ -arithmetic a multiplication diagram illustrating multiplication by a non-zero element in the arithmetic will consist of cycles if  $m$  is a prime number. The following

sequence of theorems which occur as problems in Dynkin and Uspenskii (4) establishes this conjecture.

Theorem 2. If  $a$  is a non-zero number in  $p$ -arithmetic, then in the diagram for multiplication by  $a$ , no number has two arrows leading to it.

Proof: Suppose  $b \in p$ -arithmetic and that two arrows lead to  $b$ . Then there exist distinct numbers  $x, y \in p$ -arithmetic such that  $ax=b$  and  $ay=b$ ; hence  $ax=ay$ . Therefore  $ax-ay=0$  and thus  $a(x-y)=0$ . Theorem 1 together with the fact that  $a \neq 0$  implies that  $x-y=0$ , but this is impossible if  $x$  and  $y$  are distinct. Thus there exists no number  $b$  in  $p$ -arithmetic which has two arrows leading to it.

Theorem 3. Let  $a$  and  $b$  be numbers in  $p$ -arithmetic with  $a \neq 0$ . Then every equation of the form  $ax=b$  has a unique solution.

Proof: If the equation  $ax=b$  has a solution, then it is necessarily unique since otherwise in the diagram for multiplication by  $a$ , there would be two arrows leading to  $b$  in violation of Theorem 2. To establish the existence of a solution, it suffices to let  $x$  assume each of the values  $0, 1, 2, \dots, p-1$  and consider the products  $a \cdot x$ . As  $x$  ranges over the set  $T = \{0, 1, \dots, p-1\}$ ,  $a \cdot x$  must also take on all the values in  $T$ . If this were not the case, there would exist  $c \in T$  such that for  $x_1 \in T$  and  $x_2 \in T$ ,  $x_1 \neq x_2$ ,  $ax_1 = c$  and  $ax_2 = c$ , but this is impossible by Theorem 2. Thus it

must be concluded that  $ax=b$  has a unique solution.

Theorem 4. Let  $a$  be an arbitrary non-zero number in  $p$ -arithmetic. Then the diagram for multiplication by  $a$  consists of cycles and all the cycles (except the zero-cycle) have the same length.

Proof: It is obvious that since  $a \cdot 0 = 0$  then the numbers  $\{0, a \cdot 0\}$  constitute a cycle. If  $b \neq 0$  then one must examine the sequence  $\{b, ab, a^2b, \dots\}$ . Either all the elements of this set are different or else there must be numbers which are repeated. The former alternative is impossible since all the numbers in this sequence are numbers in  $p$ -arithmetic which contains only  $p$  elements. If  $a^n \cdot b$  is the first number in the sequence which is a repeat of some previous number, then  $a^n \cdot b = b$  for if  $a^n \cdot b = a^i \cdot b$  with  $i < n$  then  $a \cdot (a^{i-1} \cdot b) = a^i \cdot b = a \cdot (a^{n-1} \cdot b)$  where  $a^{n-1} \cdot b \neq a^{i-1} \cdot b$ . Thus two distinct arrows go to  $a^i \cdot b$  which by Theorem 2 is impossible. Hence the numbers  $\{b, a \cdot b, a^2 \cdot b, \dots, a^n \cdot b\}$  constitute a cycle.

To show that all non-zero cycles have the same length, it will be sufficient to show that they all have the same length as the cycle containing 1. If  $b \neq 0$  and if  $\{1, a, a^2, \dots, a^n\}$  is the cycle containing 1, then the set  $\{b, ab, a^2b, \dots, a^n \cdot b\}$  is also a cycle since  $a^n \cdot b = 1 \cdot b = b$  and if  $a^i \cdot b = b$ , then  $a^i = 1$  which implies that  $i$  is a multiple of  $n$ . Hence  $\{b, a \cdot b, a^2 \cdot b, \dots, a^n \cdot b\}$  is a cycle



containing  $b$  and having the same length as the  $l$ -cycle.

Since  $b$  was an arbitrary non-zero number, it may be concluded that all of these cycles have the same length.

The following basic theorem of elementary number theory is an immediate consequence of Theorem 4.

**Theorem 5.** (Fermat's Theorem) If  $p$  is a prime and  $p \nmid a$  then  $p \mid (a^{p-1} - 1)$ .

**Proof:** Since the diagram for multiplication by  $a$  consists of cycles and since by the previous theorem all these cycles have the same length,  $s$ , then the number of cycles not containing zero is  $n = (p-1)/s$ . Thus  $a^s = 1 \implies (a^s)^n = 1^n = 1 \implies a^{p-1} = 1$ . Therefore  $a^{p-1} - 1 = 0$  and  $p \mid (a^{p-1} - 1)$ .

By Theorem 3 if  $a \neq 0$  then every equation of the form  $ax = 1$  has a unique solution in  $p$ -arithmetic. Thus Theorem 3 insures that every non-zero number in  $p$ -arithmetic has a unique multiplicative inverse.

Basic to the following theorem is the observation that  $1$  and  $p-1$  are multiplicative self-inverses in  $p$ -arithmetic and that  $1$  and  $p-1$  are additive inverses.

**Theorem 6.** (Wilson's Theorem) If  $p$  is a prime number then  $(p-1)! + 1$  is divisible by  $p$ .

**Proof:** The theorem is immediately apparent if  $p=2$ ; it may therefore be assumed that  $p > 2$ . Then  $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$  and in this product  $1$  and  $p-1$  are multiplicative self-inverses.

The product  $2 \cdot 3 \cdot \dots \cdot (p-2) = 1$  since the multiplicative inverse of each element in the set  $S = \{2, 3, \dots, (p-2)\}$  is also in  $S$ , and the product  $2 \cdot 3 \cdot \dots \cdot (p-2)$  may be written as the product of  $(p-3)/2$  factors each of which is a number in  $p$ -arithmetic multiplied by its multiplicative inverse. Consequently,  $(p-1) \cdot 1 = (p-1)$  or  $(p-1) \cdot 1 = (p-1) + 1 = 0$  and it follows that  $(p-1) \cdot 1$  is divisible by  $p$ .

Theorem 7. (Converse of Wilson's Theorem). If  $m$  divides  $(m-1) \cdot 1$ , then  $m$  is a prime number.

Proof: If  $m$  is not prime, then there exists  $d$ ,  $1 < d < m$  such that  $d \mid m$ . Also  $d \mid (m-1) \cdot 1$  since it is one of the factors in the product  $(m-1) \cdot 1$ . Hence  $d \mid (m-1) \cdot 1 + 1$  since  $d \mid m$  and  $m \mid (m-1) \cdot 1 + 1$ . Therefore  $d \mid [(m-1) \cdot 1 + 1 - (m-1) \cdot 1]$ , but this implies that  $d \mid 1$  which is impossible since  $1 < d$ . Consequently, if  $m \mid (m-1) \cdot 1 + 1$ , then  $m$  must be a prime number.

In 5-arithmetic  $1^2 = 1$  and  $4^2 = 1$ , but there is no number in 5-arithmetic satisfying the equation  $x^2 = 2$ . It is therefore obvious that in  $m$ -arithmetic the equation  $x^n = a$  may or may not have solutions. One is naturally interested in knowing when this equation has solutions and in the number of solutions it has if any do exist. Most number theory texts contain partial answers to these questions. As far as the writer has been able to determine, however, the following theorem is an addition to the list of partial answers.

Theorem 8. If  $x^n = a$  has solutions in  $m$ -arithmetic, then the number of solutions divides  $\phi(m)$  where  $\phi(m)$  denotes Euler's  $\phi$ -function.

To facilitate the proof of the theorem, certain standard theorems of number theory will be employed. These theorems are stated below without proof, but, in each case, the source of a proof is cited.

Theorem 9. Long (7). The linear congruence  $ax \equiv b \pmod{m}$  is solvable if and only if  $d \mid b$  where  $d = (a, m)$ . If there are any solutions, then there are precisely  $d$  incongruent solutions.

Theorem 10. Niven and Zuckerman (11). If  $p$  is a prime and  $(a, p) = 1$ , then the congruence  $x^n \equiv a \pmod{p}$  has  $(n, p-1)$  solutions or no solutions according as  $a^{(p-1)/(n, p-1)} \equiv 1 \pmod{p}$  or  $a^{(p-1)/(n, p-1)} \not\equiv 1 \pmod{p}$ .

Theorem 11. Long (7). Let  $f(x)$  be a polynomial with integral coefficients, let  $p$  be a prime, and let  $\alpha \geq 2$  be an integer. Then,  $x_0$  is a solution of  $f(x) \equiv 0 \pmod{p}$  if and only if

$$x_0 = r + y_0 p^{\alpha-1}$$

where  $r$  is a solution of  $f(x) \equiv 0 \pmod{p}$  and  $y_0$  is a solution of

$$\frac{f(x)}{p^{\alpha-1}} + y f'(r) \equiv 0 \pmod{p}.$$

Theorem 12. Chinese Remainder Theorem. Long (7). If

$(m_i, m_j) = 1$  for  $i \neq j$  then the system

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

-----

$$x \equiv c_r \pmod{m_r}$$

is solvable with a unique solution modulo  $m$  where  $m = \prod_{i=1}^r m_i$ .

Theorem 13. Long (7). Let  $f(x) = \sum_{k=0}^n c_k x^k$  where  $c_0, c_1, \dots,$

$c_n$  are integers. If  $a \equiv b \pmod{m}$ , then  $f(a) \equiv f(b) \pmod{m}$ .

Since the number of solutions of the equation  $x^n = a$  in  $m$ -arithmetic is the same as the number of incongruent solutions of  $x^n \equiv a \pmod{m}$ , the latter notation will be employed in proving Theorem 8 in order to facilitate the use of the preceding theorems.

Proof of Theorem 8. Two cases will be considered.

Case I. If  $m = p^k$  where  $p$  is a prime and  $k$  is a natural number, the proof will be by induction on  $k$ .

(a) If  $k=1$ , if  $(a, p) = 1$ , and if  $x^n \equiv a \pmod{p}$  has solutions, they are  $(n, p-1)$  in number by Theorem 10. However,  $\phi(p) = p-1$  and therefore the number of solutions divides  $\phi(p)$ . If  $(a, p) = 1$  only one solution exists,  $x_0 \equiv 0 \pmod{p}$ . Therefore, if  $x^n \equiv a \pmod{p}$  has solutions, their number divides  $\phi(p)$ .

(b) Assume that if  $x^n \equiv a \pmod{p^k}$  has solutions, then the

number of solutions divides  $\phi(p^k)$ ,  $k=1, 2, \dots, j$ .

(c) By Theorem 11  $x_0$  will be a solution of  $x^n \equiv a \pmod{p^{j+1}}$  if and only if

$$x_0 = r + y_0 p^j$$

where  $r$  is a solution of

$$(A) \quad x^n \equiv a \pmod{p^{j+1}}$$

and  $y_0$  is a solution of

$$(B) \quad \frac{r^n - a}{p^j} + n r^{n-1} y_0 \equiv 0 \pmod{p}.$$

Thus  $x^n \equiv a \pmod{p^{j+1}}$  has solutions if and only if both (A) and (B) have solutions. Now by Theorem 9, if (B) has solutions, it will have either  $p$  incongruent solutions or one solution. By (b), if (A) has solutions, their number will divide  $\phi(p^j) = p^{j-1}(p-1)$ . Let  $N_0$  be the number of solutions of (A) and let  $N_1$  be the number of solutions of  $x^n \equiv a \pmod{p^{j+1}}$ , if solutions exist. Then  $N_1 = N_0$  or  $N_1 = p \cdot N_0$  depending upon whether (B) has one or  $p$  solutions. However, since  $\phi(p^{j+1}) = p\phi(p^j)$  and since  $N_0 \mid \phi(p^j)$ , in either case  $N_1 \mid \phi(p^{j+1})$ .

Case II.  $(m = \prod_{i=1}^k p_i^{\alpha_i})$ .

Clearly in this case  $x_0$  is a solution of  $x^n \equiv a \pmod{m}$  if and only if  $x_0$  is a solution of  $x^n \equiv a \pmod{p_i^{\alpha_i}}$  for each  $i$ . In fact, if  $x_i$ ,  $i=1, \dots, k$  are solutions of the congruences  $x^n \equiv a \pmod{p_i^{\alpha_i}}$ , the Chinese Remainder Theorem

guarantees a unique solution,  $x_0$ , of the system  $x \equiv x_i \pmod{p_i^{\alpha_i}}$ ,  $i=1, \dots, k$ , and by Theorem 13  $x_0^n \equiv a \pmod{p_i^{\alpha_i}}$  for every  $i$ ; hence  $x_0^n \equiv a \pmod{m}$ . Thus every combination of solutions of the congruences  $x^n \equiv a \pmod{p_i^{\alpha_i}}$ ,  $i=1, \dots, k$  yields a distinct solution of  $x^n \equiv a \pmod{m}$ . Therefore, if

$N_i$  denotes the number of solutions of  $x^n \equiv a \pmod{p_i^{\alpha_i}}$ , then  $N = \prod_{i=1}^k N_i$ . Hence, since  $N_i \mid \phi(p_i^{\alpha_i})$  and since  $\phi(m) = \prod_{i=1}^k \phi(p_i^{\alpha_i})$ , it follows that  $N \mid \phi(m)$ .

### M-Adic Numbers

Addition, subtraction, and multiplication in elementary arithmetic can generally be performed in a straightforward manner with near-complete confidence at every step. This may not be the case with division, however, for in this operation there is quite often a certain amount of guesswork involved. For example,  $1241 \div 17 = 73$ , but, as division is customarily performed, one might not see immediately that the ten's digit in the quotient is 7; a moderate amount of trial and error might be involved. This trial and error may be eliminated, however, by performing the division in the following manner:

- (1) Calculate the multiplicative inverse of the unit's digit of the divisor in 10-arithmetic. In the example under consideration,  $7^{-1} = 3$  since  $7 \cdot 3 = 1$ .

For the sake of convenience, this multiplicative inverse may be recorded as a superscript of the divisor.

- (2) Obtain the unit's digit of the quotient by multiplying the inverse obtained in the previous step by the unit's digit of the dividend. In dividing 1241 by 17, all the information obtained thus far is contained in the following array.

$$\begin{array}{r} 3 \\ \hline 1241 \boxed{17^3} \end{array}$$

- (3) Multiply the divisor by the unit's digit of the quotient and subtract the product from the dividend as in ordinary arithmetic. The continuation of the above array would then appear as

$$\begin{array}{r} 3 \\ \hline 1241 \boxed{17^3} \\ \hline 51 \\ \hline 119 \end{array}$$

- (4) Obtain the ten's digit of the quotient by multiplying, in 10-arithmetic, the last digit of the remainder obtained in (3) by the inverse obtained in (1). The example of (3) then becomes

$$\begin{array}{r} 73 \\ \hline 1241 \boxed{17^3} \\ \hline 51 \\ \hline 119 \end{array}$$

- (5) Multiply the divisor by the ten's digit obtained

in (4) and subtract from the remainder obtained in (3). The continuation of the example then appears as

$$\begin{array}{r}
 73 \\
 1241 \overline{) 17^3} \\
 \underline{51} \\
 119 \\
 \underline{119} \\
 0
 \end{array}$$

and, since the remainder in this step is zero, the division process is complete.

To help illustrate this method of division, three additional examples follow.

$$\begin{array}{r}
 32 \\
 1952 \overline{) 61^1} \\
 \underline{122} \\
 183 \\
 \underline{183} \\
 \underline{\quad}
 \end{array}$$

$$\begin{array}{r}
 26 \\
 1378 \overline{) 53^7} \\
 \underline{318} \\
 106 \\
 \underline{106} \\
 \underline{\quad}
 \end{array}$$

$$\begin{array}{r}
 47 \\
 1363 \overline{) 53^7} \\
 \underline{203} \\
 116 \\
 \underline{116} \\
 \underline{\quad}
 \end{array}$$

The reader may have observed by now that the process of division may not always be as easy as it was in the above examples. If, for example, the divisor is 34, the method is not even applicable since 4 has no multiplicative inverse in 10-arithmetic. One might, of course, divide the divisor and dividend by 2 so as to obtain a divisor of 17 whose last digit has 3 as a multiplicative inverse. He would have to use the usual method of dividing by 2, however, since 2 itself has no multiplicative inverse in 10-arithmetic.



Another difficulty which might be encountered is that the divisor may not divide into the dividend an integral number of times. This is illustrated by the next example.

$$\begin{array}{r} 71 \\ 13 \overline{) 3^7} \\ \underline{3} \\ 1 \\ \underline{21} \end{array}$$

This array indicates that the next step is to subtract 21 from 1, or more precisely, 210 from 10 leaving a remainder of -200. It is perhaps not too surprising that 13 is indeed equal to  $3.71 + (-200)$ .

The previous example is now continued by actually performing the succeeding subtractions and divisions. In this extended array -2 is written as  $-10+8$  using the notation  $\bar{1}8$  for  $-10+8$ .

$$\begin{array}{r} \dots 66671 \\ 13 \overline{) 3^7} \\ \underline{3} \\ 1 \\ \underline{21} \\ \bar{1}8 \\ \underline{\bar{1}8} \\ \bar{1}8 \\ \underline{\bar{1}8} \\ \bar{1}8 \\ \underline{\bar{1}8} \\ \bar{1}8 \end{array}$$

If  $13 \div 3 = \dots 66671$  then this quotient must obviously be a "different kind of number." The plausibility of  $\dots 66671$  as the quotient of  $13 \div 3$  might be enhanced somewhat if  $\dots 66671 \times 3 = 13$ . The following array indicates

that this appears to be true in a certain sense.

$$\begin{array}{r} \dots 66671 \\ \times \quad \quad 3 \\ \hline \dots 00013 \end{array}$$

The new kind of number which was encountered in the above problem will be called a 10-adic number. More generally, if  $m$  is used as a base, then a number with an infinite number of digits to the left of the decimal will be called an  $m$ -adic number.

If  $n$  is a whole number with base ten representation  $a_k a_{k-1} \dots a_2 a_1$ , then one could associate  $n$  with the 10-adic number  $\dots 000 a_k a_{k-1} \dots a_2 a_1$ , thereby obtaining a one-to-one correspondence between the whole numbers and a certain subset of the 10-adic numbers. Any whole number greater than 1 could be used as the base, but there is some advantage in using a prime base. There could, for example, be no difficulty encountered in dividing one integer by another using the above method if both were expressed in the prime base  $p$ , since multiplicative inverses always exist in  $p$ -arithmetic. Dynkin and Uspenskii (4) give an added reason for considering a prime base by showing that there exists a non-zero 10-adic number with no multiplicative inverse.

A prime base,  $p$ , is used almost exclusively in the following chapter and the associated  $p$ -adic numbers are

developed as a completion of the rational field. Following their development is a brief discussion of some of their most important properties.

## CHAPTER III

### VALUATIONS

The real numbers are often developed from the rational numbers through the use of Cauchy sequence of rationals. Such, for example, is the method used in The Number System by Thurston (12). In questions concerning convergence of these sequences, the metric,  $d$ , defined by  $d(a,b)=|a-b|$  is employed. One of the primary objectives of this chapter is to show that one can employ a different metric and obtain an entirely different completion of the rational field. Valuations are introduced as a first step in this endeavor.

Definition 1. A valuation of a field,  $F$ , is a function  $\phi$  from  $F$  to the real field,  $R$ , such that the following properties hold.

- (1)  $\forall a \in F, \phi(a) \geq 0$  and  $\phi(a)=0$  if and only if  $a=0$ .
- (2)  $\forall a \in F, \text{ and } \forall b \in F, \phi(ab)=\phi(a) \cdot \phi(b)$ .
- (3) (Triangle inequality)  $\forall a \in F \text{ and } \forall b \in F, \phi(a+b) \leq \phi(a) + \phi(b)$ .

The following additional properties of a valuation follow rather easily from the above definition.

- (1)  $\phi(\pm 1) = 1$
- (2)  $\forall a \in F, \phi(-a) = \phi(a)$
- (3)  $\forall a \in F$  and  $\forall b \in F, |\phi(a) - \phi(b)| \leq \phi(a \pm b)$ .
- (4)  $\forall a \in F$  and  $\forall b \in F, b \neq 0, \phi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)}$

Hereafter this paper will be concerned solely with valuations of the rational field,  $\mathbb{Q}$ . It will be established that every valuation of the field,  $\mathbb{Q}$ , is one of the following four types of valuations.

- (1) Absolute value (denoted hereafter by  $||$ ).
- (2)  $||^\alpha$  where  $\alpha$  is a real number such that  $0 < \alpha \leq 1$ .
- (3) The trivial valuation  $\phi: \mathbb{Q} \rightarrow \mathbb{R}$  such that  $\phi(0) = 0$  and  $\phi(a) = 1$  if  $a \neq 0$ .
- (4) A  $p$ -adic valuation which will be defined below.

The reader will be able to agree easily that (1) and (3) are indeed valuations of  $\mathbb{Q}$ . Both (2) and (4) will be investigated in this paper.

It is readily apparent that  $||^\alpha$  possesses properties (1) and (2) of Definition 1. That  $\forall a \in \mathbb{Q}$  and  $\forall b \in \mathbb{Q}, |a+b|^\alpha \leq |a|^\alpha + |b|^\alpha$  is perhaps not quite as clear unless  $a=0$  or  $b=0$ , but can be established through the following sequence of observations under the assumption that  $|a| \leq |b| \neq 0$ .

$$\begin{aligned}
 |a+b|^\alpha &\leq (|a| + |b|)^\alpha \\
 &= \left[ |b| \left( \frac{|a|}{|b|} + 1 \right) \right]^\alpha \\
 &= |b|^\alpha \left( \frac{|a|}{|b|} + 1 \right)^\alpha
 \end{aligned}$$

$$\begin{aligned}
&\leq |b|^\alpha \left( \frac{|a|}{|b|} + 1 \right) \\
&\leq |b|^\alpha \left[ \left( \frac{|a|}{|b|} \right)^\alpha + 1 \right] \\
&= |b|^\alpha \left( \frac{|a|^\alpha}{|b|^\alpha} + 1 \right) \\
&= |a|^\alpha + |b|^\alpha
\end{aligned}$$

It should be observed that the assumption  $|a| \leq |b| \neq 0$  is not really restrictive since there is complete symmetry in  $a$  and  $b$  and if  $a=0$  or  $b=0$ , the inequality  $|a+b|^\alpha \leq |a|^\alpha + |b|^\alpha$  holds trivially. Hence  $|\cdot|^\alpha$  is a valuation of  $\mathbb{Q}$ .

An important preliminary to the definition of a  $p$ -adic valuation is the observation that if  $p$  is a fixed prime and  $q$  is a nonzero rational number, then there exist integers  $n$ ,  $a$ , and  $b$  such that  $p \nmid a$ ,  $p \nmid b$ , and  $q = p^n \cdot \frac{a}{b}$ . The expression  $p^n \cdot \frac{a}{b}$  will be called a  $p$ -representation of  $q$ .

Although a  $p$ -representation of  $q$  is not unique without further restrictions on  $a$  and  $b$ , the integer  $n$  in any  $p$ -representation of  $q$  will be unique.

Definition 2. If  $p$  is a given prime number and  $\alpha$  is a fixed real number such that  $0 < \alpha < 1$ , the function  $\phi_p: \mathbb{Q} \rightarrow \mathbb{R}$  defined as follows will be called a  $p$ -adic valuation of  $\mathbb{Q}$ .

$$(1) \quad \phi_p(0) = 0$$

$$(2) \quad \text{If } q \neq 0, \phi_p(q) = \alpha^n \text{ where } n \text{ is the exponent of } p \text{ in}$$

a  $p$ -representation of  $q$ .

It is apparent that the function  $\phi_p$  of the preceding

definition has the first property stipulated by Definition 1.

If either  $q=0$  or  $r=0$  it is equally apparent that

$\phi_p(qr) = \phi_p(q) \cdot \phi_p(r)$  and that  $\phi_p(q+r) \leq \phi_p(q) + \phi_p(r)$ . If both

$a$  and  $b$  are non-zero rational numbers with  $p$ -representations

$q = p^n \cdot \frac{a}{b}$  and  $r = p^m \cdot \frac{c}{d}$ , then  $q \cdot r = p^{n+m} \cdot \frac{ac}{bd}$ . Furthermore,  $p \nmid ac$

and  $p \nmid bd$ . Therefore,  $\phi_p(q \cdot r) = \alpha^{n+m} = \alpha^n \cdot \alpha^m = \phi_p(q) \cdot \phi_p(r)$ . If

$\phi_p(q) \neq \phi_p(r)$  it may be assumed without loss of generality that

$\phi_p(q) < \phi_p(r)$  or equivalently that  $n > m$ , then  $q+r = \frac{p^n ad + p^m bc}{bd}$

$= p^m \frac{p^{n-m} ad + bc}{bd}$  and since  $p$  divides neither  $bd$  nor  $(p^{n-m} ad + bc)$ ,

$\phi_p(q+r) = \alpha^m = \phi_p(r) = \max[\phi_p(q), \phi_p(r)]$ . If  $\phi_p(q) = \phi_p(r) = \alpha^n$  then

$\phi_p(q+r) = \alpha^k$ ,  $k \geq n$ , if  $q \neq -r$ ; if  $q = -r$ ,  $\phi_p(q+r) = 0$ . In any event,

the above results may be summarized in the inequality

$\phi_p(q+r) \leq \max[\phi_p(q), \phi_p(r)]$ , which in turn implies the

triangle inequality. Thus it has been shown that  $\phi_p$  is a

valuation of  $\mathbb{Q}$ .

**Definition 3.** A valuation  $\phi$  for which  $\phi(q+r) \leq \max[\phi(q), \phi(r)]$

is said to be a non-Archimedean valuation.

A complete description of all possible valuations of the rational field  $\mathbb{Q}$  is contained in the following theorem which is taken with some modification from Number Theory by Borevich and Shafarevich (2).

**Theorem 1.** (Ostrowski's Theorem). Every non-trivial valuation

of the field of rational numbers is of the form  $|\cdot|^\alpha$  with

$0 < \alpha \leq 1$  or is a  $p$ -adic valuation for some prime number,  $p$ .

Proof: If  $\phi$  is a non-trivial valuation of the field  $Q$ , then for every natural number,  $n$ ,  $\phi(n) \leq 1$  or else there exists a natural number  $m > 1$  such that  $\phi(m) > 1$ .

If the latter case holds, there must exist a real number,  $\alpha$ ,  $0 < \alpha \leq 1$  such that

$$\phi(m) = m^\alpha$$

since in all cases

$$\phi(n) = \phi(1+1+\dots+1) \leq \phi(1) + \phi(1) + \dots + \phi(1) = n.$$

Any arbitrary natural number  $N$  may be represented as a polynomial in  $m$  with integral coefficients as follows.

$$N = a_0 + a_1 m + a_2 m^2 + \dots + a_{k-1} m^{k-1}$$

with  $0 \leq a_i \leq m-1$  for  $0 \leq i \leq k-1$  and  $m^{k-1} \leq N < m^k$ .

Thus

$$\phi(N) \leq \phi(a_0) + \phi(a_1) m^\alpha + \phi(a_2) m^{2\alpha} + \dots + \phi(a_{k-1}) m^{(k-1)\alpha}$$

and since  $\phi(a_i) \leq a_i \leq m-1$ ,  $0 \leq i \leq k-1$

$$\begin{aligned} \phi(N) &\leq (m-1) (1 + m^\alpha + m^{2\alpha} + \dots + m^{(k-1)\alpha}) \\ &= (m-1) \frac{m^{k\alpha} - 1}{m^\alpha - 1} \\ &< (m-1) \frac{m^{k\alpha}}{m^\alpha - 1} \\ &= \frac{(m-1) m^\alpha}{m^\alpha - 1} m^{(k-1)\alpha} \\ &\leq \frac{(m-1) m^\alpha}{m^\alpha - 1} N^\alpha = CN^\alpha \end{aligned}$$

where  $C$  is a constant independent of  $N$ . If  $t$  is any natural number, then



$$[\phi(N)]^t = \phi(N^t) \leq CN^t \alpha$$

whence

$$\phi(N) \leq \sqrt[t]{CN} \alpha$$

and upon letting  $t \rightarrow \infty$  it follows that

$$\phi(N) \leq N^\alpha.$$

On the other hand since  $m^{k-1} \leq N < m^k$  there exists an integer  $b$  with  $0 < b \leq m^k - m^{k-1}$  such that  $N = m^k - b$ . Consequently,

$$\begin{aligned} \phi(N) &= \phi(m^k - b) \geq \phi(m^k) - \phi(b) \\ &= [\phi(m)]^k - \phi(b) \\ &= m^{\alpha k} - \phi(b) \end{aligned}$$

But  $\phi(b) \leq b^\alpha \leq (m^k - m^{k-1})^\alpha$ . Hence

$$\begin{aligned} \phi(N) &\geq m^{\alpha k} - (m^k - m^{k-1})^\alpha \\ &= m^{\alpha k} - \left[ m^k \left( 1 - \frac{1}{m} \right) \right]^\alpha \\ &= \left[ 1 - \left( 1 - \frac{1}{m} \right)^\alpha \right] m^{\alpha k} \\ &\geq \left[ 1 - \left( 1 - \frac{1}{m} \right) \right]^\alpha N^\alpha \\ &= C_1 N^\alpha \text{ where } C_1 \text{ is independent} \end{aligned}$$

of  $N$ .

Consequently, if  $t$  is an arbitrary natural number,

$$[\phi(N)]^t = \phi(N^t) = C_1 N^t \alpha \text{ and } \phi(N) \geq \sqrt[t]{C_1} N^\alpha.$$

By letting  $t$  tend to infinity it follows that

$$\phi(N) \geq N^\alpha.$$

Therefore  $\phi(n) = N^\alpha$  for every natural number,  $N$ .

For any rational number,  $q$ , there exist natural numbers  $N_1$  and  $N_2$  such that  $q = \frac{N_1}{N_2}$ .

$$\text{Hence } \phi(q) = \frac{\phi(N_1)}{\phi(N_2)} = \frac{N_1^\alpha}{N_2^\alpha} = q.$$

Consequently, if there is one natural number,  $m$ , such that  $\phi(m) > 1$  then  $\phi = | \cdot |^\alpha$  for some  $\alpha$  with  $0 < \alpha \leq 1$ .

There remains now the case in which  $\phi(n) \leq 1$  for every natural number  $n$ . In this case there must exist some prime number  $p$  such that  $\phi(p) < 1$  for if  $\phi(p) = 1$  for every prime number,  $p$ , then  $\phi(n) = 1$  for every non-zero integer and hence for every non-zero rational number. This would, however, contradict the assumption that  $\phi$  is non-trivial.

If there also exists a prime  $q \neq p$  with  $\phi(q) < 1$  then integers  $k$  and  $d$  may be found such that

$$[\phi(p)]^k < 1/2 \text{ and } [\phi(q)]^d < 1/2.$$

Since  $(p^k, q^d) = 1$  there exist integers  $r$  and  $s$  such that  $rp^k + sq^d = 1$ . Hence

$$\begin{aligned} 1 = \phi(1) = \phi(rp^k + sq^d) &\leq \phi(r)\phi(p^k) + \phi(s)\phi(q^d) \\ &\leq 1 \cdot \phi(p^k) + 1 \cdot \phi(q^d) < 1/2 + 1/2 = 1 \end{aligned}$$

This contradiction points out that there can be only one prime,  $p$ , for which  $\phi(p) < 1$  and that  $\phi(q) = 1$  for every other prime number,  $q$ . As a result  $\phi(n) = 1$  for every integer,  $n$ , such that  $(n, p) = 1$ . Therefore, if  $r$  is any non-zero rational number with  $p$ -representation  $r = p^m \frac{a}{b}$  then

$$\phi(r) = \phi(p^m) \cdot \frac{\phi(a)}{\phi(b)} = \phi(p)^m \cdot \frac{1}{1} = \alpha^m$$

and  $\phi$  is thus a  $p$ -adic valuation of  $\mathbb{Q}$ . It has consequently been established that every valuation of  $\mathbb{Q}$  is of the form  $|\cdot|^\alpha$  with  $0 < \alpha \leq 1$  or is else a  $p$ -adic valuation for some prime,  $p$ .

### Metrics

Definition 4. A metric on a set,  $S$ , is a function  $d: S \times S \rightarrow \mathbb{R}$  with the following properties.

- (a)  $\forall x \in S$  and  $\forall y \in S$ ,  $d(x, y) \geq 0$  and  $d(x, y) = 0$  if and only if  $x = y$ .
- (b)  $\forall x \in S$  and  $\forall y \in S$ ,  $d(x, y) = d(y, x)$ .
- (c) (Triangle inequality)  $\forall x \in S, \forall y \in S$ , and  $\forall z \in S$ ,  
 $d(x, z) \leq d(x, y) + d(y, z)$ .

Theorem 2. Any valuation of a field,  $F$ , induces a metric on  $F$ .

Proof: Let  $\phi$  be a valuation of the field  $F$  and define

$d_\phi: F \times F \rightarrow \mathbb{R}$  as follows:  $\forall (x, y) \in F \times F$ ,  $d_\phi(x, y) = \phi(x - y)$ . That  $d_\phi$  has properties (a) and (b) of Definition 4 is immediately apparent. Property (c) follows rather easily since:

$$d_\phi(x, z) = \phi(x - z) = \phi[(x - y) + (y - z)] \leq \phi(x - y) + \phi(y - z) = d_\phi(x, y) + d_\phi(y, z).$$

Consequently,  $d_\phi$  is a metric on  $F \times F$ .

If  $\phi$  is a non-Archimedean valuation, then the associated metric,  $d_\phi$ , has the property that  $d_\phi(x, z) \leq \max[d_\phi(x, y), d_\phi(y, z)]$ .

Such a metric will be said to have the ultra-metric property and will be called a non-Archimedean metric.

### P-adic Numbers

Definition 5. A sequence  $\{x_n\}$  of elements of a field,  $F$ , is said to converge to the element  $a \in F$  in the metric,  $d$ , if and only if for every real  $\epsilon > 0$  there exists a positive integer  $N$ , such that for all  $n > N$ ,  $d(x_n, a) < \epsilon$ . That  $\{x_n\}$  converges to  $a$  will be denoted by  $\{x_n\} \rightarrow a$  or by  $\lim_{n \rightarrow \infty} x_n = a$ .

Definition 6. A sequence  $\{x_n\}$  is called a Cauchy sequence with respect to the metric,  $d$ , if and only if for every real  $\epsilon > 0$  there exists a positive integer,  $N$ , such that  $d(x_m, x_n) < \epsilon$  whenever  $m > N$  and  $n > N$ .

Definition 7. A field  $F$  is said to be complete with respect to the metric,  $d$ , if and only if every Cauchy sequence in  $F$  converges in the metric,  $d$ , to an element of  $F$ .

Theorem 2. A sequence  $\{x_n\}$  converges in the metric,  $d$ , to at most one limit.

Proof: If  $\{x_n\} \rightarrow r$  and  $\{x_n\} \rightarrow s$  with  $r \neq s$  then if  $\epsilon = 1/3d(r, s)$  there exist  $N_1$  and  $N_2$  such that for all  $n > N_1$   $d(x_n, r) < \epsilon$  and for all  $n > N_2$   $d(x_n, s) < \epsilon$ . Therefore, if  $n > \max(N_1, N_2)$  then  $d(x_n, r) + d(x_n, s) < 2\epsilon = 2/3 d(r, s)$ . But  $d(r, s) \leq d(x_n, r) + d(x_n, s) < 2/3 d(r, s)$  which is impossible. Consequently,

$\{x_n\}$  converges to at most one limit.

It is a well known fact that the rational field,  $Q$ , is not complete with respect to the absolute value metric. This is established for example, in The Structure of the Real Number System by Cohen and Ehrlich (3). The following example from Borevich and Shafarevich (2) shows that it is also possible to construct Cauchy sequences of rational numbers with respect to a p-adic metric which do not converge to a rational number. This is accomplished by inductively constructing solutions to the congruences

$$x^2 \equiv 2 \pmod{7^n}.$$

If  $n=1$  the congruence has the solution

$$x_0 \equiv 3 \pmod{7}.$$

Assuming now that  $x_{k-1}$  is a solution to

$$x^2 \equiv 2 \pmod{7^k}$$

where  $k$  is an arbitrary positive integer, a solution to

$$x^2 \equiv 2 \pmod{7^{k+1}}$$

may be constructed by observing that any solution,  $x_k$ , of the latter congruence must also be a solution of

$$x^2 \equiv 2 \pmod{7^k}.$$

This suggests that one look for solutions of the form

$$x_k = x_{k-1} + t \cdot 7^k$$

Then the task is to find  $t$  satisfying the following

congruences.

$$x_k^2 = (x_{k-1} + t \cdot 7^k)^2 \equiv 2 \pmod{7^{k+1}}$$

$$x_{k-1}^2 + 2x_{k-1}t \cdot 7^k + t^2 \cdot 7^{2k} \equiv 2 \pmod{7^{k+1}}$$

$$x_{k-1}^2 - 2 + 2x_{k-1}t \cdot 7^k \equiv 0 \pmod{7^{k+1}}$$

$$M + 2x_{k-1}t \equiv 0 \pmod{7} \text{ with } x_{k-1}^2 - 2 = M \cdot 7^k$$

$$2x_{k-1}t \equiv -M \pmod{7}.$$

Since  $x_{k-1}^2 \equiv 2 \pmod{7^k}$  it follows that  $x_{k-1}^2 \equiv 2 \pmod{7}$ . Hence,

$(2x_{k-1}, 7) = 1$  and there exists an integer,  $t$ , such that

$$t \cdot 2x_{k-1} \equiv -M \pmod{7}.$$

Therefore,  $x_k = x_{k-1} + t \cdot 7^k$  is a solution of

$$x^2 \equiv 2 \pmod{7^{k+1}}$$

and a sequence  $\{x_n\}$  has been constructed inductively such

that

$$x_n^2 \equiv 2 \pmod{7^{n+1}}$$

and

$$x_n \equiv x_{n-1} \pmod{7^n}.$$

Thus, in the 7-adic metric,  $d(x_n^2, 2) \leq \alpha \frac{n+1}{7} \rightarrow 0$  as  $n \rightarrow \infty$

and if  $m \leq n$ ,  $d(x_m, x_n) \leq \alpha \frac{m+1}{7}$ . Consequently,  $\{x_n\}$  is a Cauchy

sequence converging to  $\sqrt{2}$ , and  $\mathbb{Q}$  is not complete in the

7-adic metric.

The previous example prompts one to attempt an embedding

of the rational field,  $Q$ , in a field which is complete in the  $p$ -adic metric. This can be accomplished through the following steps which differ very little from the usual steps in completing the rational field.

Let the set of all Cauchy sequences of  $Q$  (with respect to the  $p$ -adic metric,  $\phi$ ) be denoted by  $Q'$ , and define addition and multiplication in  $Q'$  as follows: if  $\bar{x} = \{x_n\}$  and  $\bar{y} = \{y_n\}$  then  $\bar{x} + \bar{y} = \{x_n + y_n\}$  and  $\bar{x} \cdot \bar{y} = \{x_n \cdot y_n\}$ .

Theorem 3. If  $\{x_n\} \in Q'$  then  $\{\phi_p(x_n)\}$  is bounded in  $R$ .

Proof: There exists  $N$  such that for all  $m, n > N$ .

$\phi_p(x_m) - \phi_p(x_n) \leq \phi_p(x_m - x_n) < 1$ . Hence for a fixed  $n_0 > N$

$\phi_p(x_m) < 1 + \phi_p(x_{n_0})$  for every  $m > N$ . Therefore, for every  $n$ ,

$\phi_p(x_n) \leq \max(\phi_p(x_1), \phi_p(x_2), \dots, \phi_p(x_n), 1 + \phi_p(x_{n_0}))$  and

$\{\phi_p(x_n)\}$  is bounded in  $R$ .

Theorem 4. If  $\bar{x} = \{x_n\} \in Q'$  and  $\bar{y} = \{y_n\} \in Q'$  then  $\bar{x} + \bar{y} \in Q'$  and

$\bar{x} \cdot \bar{y} \in Q'$ .

Proof:  $\bar{x} \in Q'$  implies that for every  $\epsilon > 0$  there exists  $N_1$

such that  $m, n > N_1$  implies that  $\phi_p(y_m - y_n) < \frac{\epsilon}{2}$  while  $\bar{y} \in Q'$

implies that for every  $\epsilon > 0$  there exists  $N_2$  such that  $m, n > N_2$

implies that  $\phi_p(x_m - x_n) < \frac{\epsilon}{2}$ . Therefore if  $m, n > \max(N_1, N_2)$

then

$$\phi_p[(x_m + y_m) - (x_n + y_n)] = \phi_p[(x_m - x_n) + (y_m - y_n)]$$

$$\leq \phi_p(x_m - x_n) + \phi_p(y_m - y_n)$$

$$< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Hence  $\bar{x} + \bar{y} \in Q'$ .

In considering the product  $\bar{x} \cdot \bar{y}$  let  $B_1$  be an upper bound of  $\{\phi_p(x_n)\}$  and let  $B_2$  be an upper bound of  $\{\phi_p(y_n)\}$ . Since  $\bar{x} \in Q'$  there exist  $N_1$  and  $N_2$  such that  $\phi_p(x_m - x_n) < \frac{\epsilon}{2B_2}$

if  $m, n > N_1$  and  $\phi_p(y_m - y_n) < \frac{\epsilon}{2B_1}$  if  $m, n > N_2$ . Thus if

$m, n > \max(N_1, N_2)$  then

$$\begin{aligned} \phi_p(x_m y_m - x_n y_n) &= \phi_p [x_m y_m - x_m y_n + x_m y_n - x_n y_n] \\ &= \phi_p [x_m (y_m - y_n) + (x_m - x_n) y_n] \\ &\leq \phi_p(x_m) \phi_p(y_m - y_n) + \phi_p(x_m - x_n) \phi_p(y_n) \\ &< B_1 \cdot \frac{\epsilon}{2B_1} + \frac{\epsilon}{2B_2} B_2 \\ &= \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \end{aligned}$$

Therefore, if  $\bar{x} \in Q'$  and  $\bar{y} \in Q'$  then  $\bar{x} \cdot \bar{y} \in Q'$ .

A relation,  $R$ , is now defined on  $Q' \times Q'$  as follows:

if  $\bar{x} = \{x_n\} \in Q'$  and  $\bar{y} = \{y_n\} \in Q'$ ,  $\bar{x} R \bar{y}$  if and only if for every

$\epsilon > 0$  there exists  $N$  such that for all  $n > N$ ,  $\phi_p(x_n - y_n) < \epsilon$ .

The relation,  $R$ , possesses the following properties.



- (1) (Reflexive) For every  $\bar{x} \in Q'$ ,  $\bar{x}R\bar{x}$ .
- (2) (Symmetric) If  $\bar{x}R\bar{y}$  then  $\bar{y}R\bar{x}$ .
- (3) (Transitive) If  $\bar{x}R\bar{y}$  and  $\bar{y}R\bar{z}$  then  $\bar{x}R\bar{z}$ .

The first two properties are immediate consequences of the definition of  $R$ . To establish the transitive property let

$\epsilon$  be an arbitrary positive real number, then there exist

$N_1$  and  $N_2$  such that if  $n > N_1$ ,  $\phi_p(x - y) < \epsilon$  and if  $n > N_2$

$\phi_p(y - z) < \epsilon$ . Hence, if  $n > \max(N_1, N_2)$ , then  $\phi_p(x - z) \leq$

$\max[\phi_p(x - y), \phi_p(y - z)] < \epsilon$  and it follows that  $\bar{x}R\bar{z}$ . The relation,  $R$ , is therefore an equivalence relation on  $Q'XQ'$ .

Definition 8. A  $p$ -adic number is an equivalence class with respect to the equivalence relation,  $R$ , defined above.

If the set of  $p$ -adic numbers is denoted by  $Q_p$  then from the definition of a  $p$ -adic number it follows that  $Q_p$  is the factor set  $Q'/R$ .

Definition 9. If  $\{x_n\} \in Q'$  the equivalence class in  $Q_p$  containing  $\{x_n\}$  is denoted by  $\overline{\{x_n\}}$ .

Definition 10. If  $\alpha \in Q_p$  and  $\beta \in Q_p$  let  $\{x_n\}$  be a sequence in  $\alpha$  and let  $\{y_n\}$  be a sequence in  $\beta$ ,  $\alpha + \beta$  and  $\alpha \cdot \beta$  are then defined by the equations:

$$(a) \alpha + \beta = \overline{\{x_n + y_n\}}$$

$$(b) \alpha \cdot \beta = \overline{\{x_n \cdot y_n\}}$$

There arises immediately the natural question of whether the sum and product just defined are independent of the choice of sequences chosen to represent  $\alpha$  and  $\beta$ . This can be answered in the affirmative by taking other representatives  $\{x'_n\}$  and  $\{y'_n\}$  of  $\alpha$  and  $\beta$  respectively. Then, if  $\epsilon > 0$  there exists  $N$  such that if  $n > N$ ,  $\phi_p(x_n - x'_n) < \frac{\epsilon}{2}$  and  $\phi_p(y_n - y'_n) < \frac{\epsilon}{2}$ .

Therefore, if  $n > N$

$$\begin{aligned} \phi_p \left[ (x_n + y_n) - (x'_n + y'_n) \right] &= \phi_p \left[ (x_n - x'_n) + (y_n - y'_n) \right] \\ &\leq \phi_p(x_n - x'_n) + \phi_p(y_n - y'_n) \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \end{aligned}$$

Hence  $\overline{\{x_n + y_n\}} = \overline{\{x'_n + y'_n\}}$ , and addition in  $Q$  is well-

defined.

By Theorem 3,  $\{\phi_p(y_n)\}$  and  $\{\phi_p(x'_n)\}$  are bounded in  $R$ . Let  $B_1$  and  $B_2$  respectively be upper bounds of  $\{\phi_p(y_n)\}$  and  $\{\phi_p(x'_n)\}$ . Then, for  $\epsilon > 0$ , there exists  $N$  such that for every  $n > N$ ,  $\phi_p(x_n - x'_n) < \frac{\epsilon}{2B_1}$  and  $\phi_p(y_n - y'_n) < \frac{\epsilon}{2B_2}$ .

Consequently,

$$\begin{aligned} \phi_p(x_n y_n - x'_n y'_n) &= \phi_p(x_n y_n - x'_n y_n + x'_n y_n - x'_n y'_n) \\ &\leq \phi_p(x_n - x'_n) \phi_p(y_n) + \phi_p(x'_n) \phi_p(y_n - y'_n) \\ &< \frac{\epsilon}{2B_1} B_1 + \frac{\epsilon}{2B_2} B_2 = \epsilon. \end{aligned}$$

Thus  $\overline{\left\{ \begin{smallmatrix} x & y \\ n & n \end{smallmatrix} \right\}} = \overline{\left\{ \begin{smallmatrix} x' & y' \\ n & n \end{smallmatrix} \right\}}$ , and multiplication in  $Q_p$  is well-defined.

As direct consequences of the preceding definitions, it follows that addition and multiplication in  $Q_p$  are both commutative and associative and that multiplication is distributive with respect to addition. Furthermore,  $\overline{\{0\}}$  and  $\overline{\{1\}}$  are respectively additive and multiplicative identities in  $Q_p$ . Since  $\phi_p(r) = \phi_p(-r)$  for every  $r \in Q$ , it follows that if  $\{x_n\}$  is Cauchy in the  $p$ -adic metric,  $d_p$ , then  $\{-x_n\}$  is also Cauchy in  $d_p$ . Therefore if  $\overline{\{x_n\}} \in Q_p$  then  $\overline{\{-x_n\}} \in Q_p$  and  $\overline{\{x_n\}} + \overline{\{-x_n\}} = \overline{\{0\}}$ . Consequently, if it can be shown that  $Q_p$  contains a multiplicative inverse for each element  $\overline{\{x_n\}} \neq \overline{\{0\}}$ , then it will have been established that  $Q_p$  is itself a field. This is accomplished in the three succeeding theorems.

**Theorem 5.** If  $\{x_n\} \in Q'$  but  $\{x_n\} \notin \overline{\{0\}}$ , then there exists a real number,  $k$ , and a natural number,  $N$ , such that

$$\phi_p(x_n) \geq k \text{ for all } n > N.$$

**Proof:** Assume, to the contrary, that for every real number,

$k$ , and for every  $N$  there exists  $s > N$  such that  $\phi_p(x_s) < k$ .

Since  $\{x_n\} \in Q'$  then for an arbitrary  $\epsilon > 0$  there exists  $N_1$

such that if  $m, n > N_1$  then  $\phi_p(x_m - x_n) < \epsilon$ . Thus if  $N = N_1$ ,

$\phi_p(x_m - x_s) < \epsilon$  for every  $m > N_1$ . But, since  $\phi_p(x_m) - \phi_p(x_s) \leq$

$\phi_p(x_m - x_s) < \epsilon$  then  $\phi_p(x_m) < \phi_p(x_s) + \epsilon < k + \epsilon$  for all  $m > N$ . As both  $k$  and  $\epsilon$  are completely arbitrary, this would require that

$\{x_n\} \in \overline{\{0\}}$  contrary to the stated hypothesis. The

existence of  $k$  and  $N$  such that  $\phi_p(x_n) \geq k$  for every  $n > N$  is

thus established.

Theorem 6. If  $\{x_n\} \in \mathbb{Q}$  and  $\{x_n\} \notin \overline{\{0\}}$  then the sequence  $\{y_n\}$

such that  $y_n = 0$  if  $x_n = 0$  and  $y_n = \frac{1}{x_n}$  if  $x_n \neq 0$  is a Cauchy

sequence in the  $p$ -adic metric.

Proof: Since  $\{x_n\} \notin \overline{\{0\}}$ , then by Theorem 5 there exist  $k$ ,

$N_1$  such that for every  $n > N_1$ ,  $\phi_p(x_n) \geq k$ . Also, since  $\{x_n\}$

is a Cauchy sequence, then for any  $\epsilon > 0$  there exists  $N_2$  such

that for all  $m, n > N_2$ ,  $\phi_p(x_m - x_n) < \epsilon \cdot k^2$ . Therefore, if

$N = \max(N_1, N_2)$  and  $m, n > N$  then

$$\begin{aligned} \phi_p(y_m - y_n) &= \phi_p\left(\frac{1}{x_m} - \frac{1}{x_n}\right) \\ &= \phi_p\left(\frac{x_n - x_m}{x_m x_n}\right) \\ &= \frac{\phi_p(x_n - x_m)}{\phi_p(x_m) \phi_p(x_n)} \\ &\leq \frac{\phi_p(x_n - x_m)}{k^2} \\ &< \frac{\epsilon k^2}{k^2} = \epsilon \end{aligned}$$

and it follows that  $\{y_n\}$  is a Cauchy sequence.

The two preceding theorems yield the following as an immediate result.

Theorem 7. If  $\{\overline{x_n}\} \in Q_p$  and  $\{\overline{x_n}\} \neq \{\overline{0}\}$  then there exists  $\{\overline{y_n}\} \in Q_p$  such that  $\{\overline{x_n}\} \cdot \{\overline{y_n}\} = \{\overline{1}\}$ .

Proof: Let  $\{\overline{y_n}\}$  be the sequence defined in Theorem 6.

Since there exist  $k$  and  $N$ , by Theorem 5, such that for all  $n > N$ ,  $\phi_p(x_n) \geq k$ , then for all  $n > N$ ,  $y_n = \frac{1}{x_n}$  and  $x_n y_n = 1$ .

Thus  $\{\overline{x_n}\} \cdot \{\overline{y_n}\} = \{\overline{x_n \cdot y_n}\} = \{\overline{1}\}$ .

By identifying the rational number  $r$  with the Cauchy sequence  $\{r\} = \{r, r, r, \dots\}$  one establishes an isomorphism between the rational field,  $Q$ , and that subset of  $Q_p$  consisting of all equivalence classes of the form  $\{\overline{r}\}$  where  $r \in Q$ .

Since each  $p$ -adic number is an equivalence class in  $Q_p$ , it may be represented by any sequence in the equivalence class. Probably the most useful representation is described in the following theorem.

Theorem 8. Every  $p$ -adic number may be represented by

$p^{-k} \{\overline{y_n}\}$  where  $k$  is a non-negative integer and  $y_n = \sum_{i=0}^n a_i p^i$

with  $0 \leq a_i < p$  for every  $i$ . (Note: This is equivalent to

saying that every  $p$ -adic number may be represented by a power series  $\sum_{i=m}^{\infty} a_i p^i$  where  $\sum_{i=m}^{\infty} a_i p^i$  is the  $p$ -adic limit of the sequence of partial sums  $\left\{ \sum_{i=m}^n a_i p^i \right\}$ .)

Proof: Long (7) proves on page 17 that every positive integer,  $x$ , can be uniquely represented in the form

$x = \sum_{i=0}^m b_i p^i$  where  $0 \leq b_i < p$ ,  $i=0, 1, \dots, m$ . If  $\{\overline{y_n}\}$  is

defined by  $y_n = \sum_{i=0}^n b_i p^i$  for  $n \leq m$  and  $y_n = \sum_{i=0}^m b_i p^i$

+  $\sum_{i=m+1}^n 0 \cdot p^i$  for  $n > m$ , then  $x$  is the  $p$ -adic limit of

$\{y_n\}$ , and  $x$  may be represented by  $x = \sum_{i=0}^{\infty} a_i p^i$  with

$a_i = b_i$ ,  $i=0, 1, \dots, m$  and  $a_i = 0$  for  $i > m$ . The required

representation is therefore possible for non-negative

integers.

If  $z$  is a negative integer, then  $z = -x$  where

$x = \sum_{i=0}^{\infty} b_i p^i$ . Since  $z+x=0$ , it follows that

$$z = (p-b_0) + \sum_{i=1}^{\infty} (p-b_i-1)p^i = \sum_{i=0}^{\infty} c_i p^i, \quad 0 \leq c_i < p.$$

Any integer may therefore be represented by a sequence  $\{y_n\}$

where  $y_n = \sum_{i=0}^n a_i p^i$  or by a power series  $\sum_{i=0}^{\infty} a_i p^i$  with

$0 \leq a_i < p$  for every  $i$ .

A rational number  $r = \frac{a}{b}$ , where  $a$  and  $b$  are integers

with  $b > 0$  and such that  $p \nmid b$ , may thus be represented by a

quotient  $\sum_{i=0}^{\infty} a_i p^i / \sum_{i=0}^n b_i p^i$  where  $a_i$  and  $b_i$  are integers

with  $0 \leq a_i < p$ ,  $0 \leq b_i < p$ , and  $b_0 \neq 0$ . Since  $b_0 \neq 0$ , there exists

an integer,  $x_0$ , with  $0 \leq x_0 < p$ , such that  $b_0 x_0 \equiv a_0 \pmod{p}$

and one may write

$$r = x_0 + \frac{\sum_{i=1}^{\infty} a_i p^{i-x_0} \cdot \sum_{i=0}^n b_i p^i}{\sum_{i=0}^n b_i p^i}.$$

In this representation,  $\sum_{i=0}^{\infty} a_i p^{i-x_0} \sum_{i=0}^n b_i p^i$  is an

integer since it is the difference of two integers.

Furthermore,  $p$  is a factor of  $\sum_{i=0}^{\infty} a_i p^{i-x_0} - \sum_{i=0}^n b_i p^i$  since since  $p \mid (a_0 - b_0 x_0)$ . Thus,

$$r = x_0 + p \frac{\sum_{i=0}^{\infty} c_i p^i}{\sum_{i=0}^n b_i p^i}, \quad 0 \leq c_i < p.$$

Similarly

$$\begin{aligned} r &= x_0 + p \left( x_1 + \frac{\sum_{i=0}^{\infty} c_i p^{i-x_1} - \sum_{i=0}^n b_i p^i}{\sum_{i=0}^n b_i p^i} \right) \\ &= x_0 + x_1 p + p^2 \frac{\sum_{i=0}^{\infty} d_i p^i}{\sum_{i=0}^n b_i p^i}. \end{aligned}$$

Continuing inductively one may write

$$r = x_0 + x_1 p + x_2 p^2 + \dots + x_n p^{n+1} \frac{\sum_{i=0}^{\infty} e_i p^i}{\sum_{i=0}^n b_i p^i}.$$

Thus  $r$  is the  $p$ -adic limit of the sequence  $\{y_n\}$  where

$$y_n = \sum_{i=0}^n x_i p^i.$$

If  $r$  is a rational number of the form  $r = p^{-k} \frac{a}{b}$  where  $p \nmid a$  and  $p \nmid b$  then by the above result  $p^k r$  is the  $p$ -adic limit of a sequence  $\{y_n\}$  where  $y_n = \sum_{i=0}^n a_i p^i$ ,  $0 \leq a_i < p$ .

Therefore  $r$  is the  $p$ -adic limit of the sequence  $\{p^{-k} y_n\}$

$\{y_n\}$ . Consequently, any rational number,  $r$ , may be represented in  $p$ -adic form as

$$r = \sum_{i=m}^{\infty} a_i p^i.$$

Finally, consider an arbitrary  $p$ -adic number  $\alpha = \overline{\{x_n\}}$ .

Since  $\{x_n\}$  is a Cauchy sequence, then for every  $\epsilon > 0$  there exists  $N_1$  such that for all  $m, n > N_1$ ,  $\phi_p(x_m - x_n) < \epsilon$ . Since  $x_m$  and  $x_n$  are rational numbers, there exist natural numbers,  $N_2$  and  $N_3$ , and non-negative integers  $a_i$  and  $b_i$  with  $0 \leq a_i < p$  and  $0 \leq b_i < p$  such that for every  $s > N_2$  and for every  $t > N_3$   $\phi_p(x_n - \sum_{i=k}^s a_i p^i) < \epsilon$  and  $\phi_p(x_m - \sum_{j=h}^t b_j p^j)$ . Now

$$\phi_p \left( \sum_{i=k}^s a_i p^i - \sum_{j=h}^t b_j p^j \right) \leq \max \left[ \phi_p \left( x_n - \sum_{i=k}^s a_i p^i \right), \phi_p(x_m - x_n), \phi_p \left( x_m - \sum_{j=h}^t b_j p^j \right) \right]$$

if  $s, t, m, n > \max(N_1, N_2, N_3)$ , and this requires that  $a_i = b_i$

for every  $i$ . If this is not the case, then let  $r$  be the

first index for which  $a_r \neq b_r$ , whence  $(a_r - b_r, p) = 1$  and

$$\phi_p \left[ (a_r - b_r) p^r + (a_{r+1} - b_{r+1}) p^{r+1} + \dots + (a_t - b_t) p^t \right] = c > 0.$$

Thus if  $\epsilon < c$ , it is not possible for  $\phi_p \left( \sum_{i=k}^s a_i p^i - \sum_{j=h}^t b_j p^j \right)$  to

be less than  $\epsilon$  unless  $a_i = b_i$  for every  $i$ . Therefore,

$$\overline{\left\{ \sum_{i=m}^n b_i p^i \right\}} = \overline{\{x_n\}}$$



and  $\alpha$  may be represented by  $p^{-k}\{y_n\}$  or by  $\sum_{i=m}^{\infty} a_i p^i$  where  $k$  is a non-negative integer and  $y_n = \sum_{i=0}^n a_i p^i$  with  $0 \leq a_i < p$ .

The representation of a  $p$ -adic number as an infinite series,  $\sum_{i=m}^{\infty} a_i p^i$ , is entirely analogous to the representation of a real number in the form  $\sum_{i=m}^{\infty} b_i \cdot 10^{-i}$ . Both series are automatically convergent in the Cauchy sense, but convergent in different metrics.

Definition 11. If a  $p$ -adic number is represented by an infinite series  $\sum_{i=m}^{\infty} a_i p^i$  with  $0 \leq a_i < p$ , it is said to be written in canonical form,

Both the real numbers and the  $p$ -adic numbers are developed as equivalence classes of Cauchy sequences of rational numbers. There is no difference at all in the method of development except that the absolute value metric is used in the development of the reals, and a  $p$ -adic metric is used in the development of the  $p$ -adic numbers. Moreover, Ostrowski's theorem implies that there are no other types of completions of the rational field since every valuation of the rational field is either a  $p$ -adic valuation or is of the form  $||^{\alpha}$  with  $0 < \alpha \leq 1$ . It is, in fact, rather easy to establish that a sequence converges with respect to  $||^{\alpha}$  if and only if it converges with respect to  $||$ . Similarly, one may establish that the  $p$ -adic limit of a sequence is

independent of the choice of  $\alpha$ ,  $0 < \alpha < 1$ , in the definition of the p-adic metric.

Although the types of completions of the rational field are rather severely limited, the number of completions is still infinite. This assertion will be established in the concluding chapter by showing that if  $p$  and  $q$  are primes with  $p \neq q$  then  $\mathbb{Q}_p$  is not isomorphic to  $\mathbb{Q}_q$  and that no  $\mathbb{Q}_p$  is isomorphic to  $\mathbb{R}$ .

## CHAPTER IV

### THE P-ADIC FIELDS

For a given prime number,  $p$ , the  $p$ -adic field  $Q_p$  was developed in the last chapter as the completion of the rational field,  $Q$ , with respect to a  $p$ -adic metric. No observation was made, however, regarding the completeness of  $Q_p$  itself. Before one can make any meaningful statement concerning the completeness of  $Q_p$ , he must, of course, have a metric defined on  $Q_p \times Q_p$ . The natural extension of the  $p$ -adic metric on  $Q \times Q$  to  $Q_p \times Q_p$  is contained in the following definition.

Definition 1. If  $\alpha \in Q_p$  and  $\beta \in Q_p$ , let  $\{x_n\} \in \alpha$  and  $\{y_n\} \in \beta$ . The function  $d: Q_p \times Q_p \rightarrow R$  defined by  $d(\alpha, \beta) = \lim_{n \rightarrow \infty} \phi_p(x_n - y_n)$  will be called a  $p$ -adic metric on  $Q_p$ .

Since the function,  $d$ , is defined on ordered pairs of equivalence classes, it should in no way depend upon the representatives of the equivalence classes. To show that  $d$  is well-defined, one has only to consider other representatives,  $\{x'_n\}$  and  $\{y'_n\}$  of  $\alpha$  and  $\beta$  respectively.

Since

$$\phi_p(x'_n - y'_n) = \phi_p(x'_n - x_n + x_n - y_n + y_n - y'_n)$$

$$\leq \max \left[ \phi_p(x'_n - x_n), \phi_p(x_n - y_n), \phi_p(y_n - y'_n) \right]$$

and

$$\begin{aligned} \phi_p(x_n - y_n) &= \phi_p(x_n - x'_n + x'_n - y'_n + y'_n - y_n) \\ &\leq \max \left[ \phi_p(x_n - x'_n), \phi_p(x'_n - y'_n), \phi_p(y'_n - y_n) \right], \end{aligned}$$

it follows that

$$\lim_{n \rightarrow \infty} \phi_p(x'_n - y'_n) \leq \lim_{n \rightarrow \infty} \phi_p(x_n - y_n)$$

and

$$\lim_{n \rightarrow \infty} \phi_p(x_n - y_n) \leq \lim_{n \rightarrow \infty} \phi_p(x'_n - y'_n)$$

because

$$\lim_{n \rightarrow \infty} \phi_p(x_n - x'_n) = \lim_{n \rightarrow \infty} \phi_p(y_n - y'_n) = 0$$

Thus the function,  $d$ , is independent of the choice of representatives of the equivalence classes. Obviously,

$d(\alpha, \beta) \geq 0$  and  $d(\alpha, \beta) = 0$  only if  $\alpha = \beta$ ; also,  $d(\alpha, \beta) = d(\beta, \alpha)$ . To establish the triangle inequality, let  $\alpha, \beta, \gamma \in Q_p$  and let  $\{x_n\} \in \alpha, \{y_n\} \in \beta$ , and  $\{z_n\} \in \gamma$ ; since

$$\phi_p(x_n - z_n) \leq \phi_p(x_n - y_n) + \phi_p(y_n - z_n)$$

for every  $n$ , then by taking limits as  $n \rightarrow \infty$  one obtains

$$d(\alpha, \gamma) \leq d(\alpha, \beta) + d(\beta, \gamma).$$

Consequently,  $d$  is indeed a metric on  $Q_p \times Q_p$ . Furthermore, on that subfield of  $Q_p$  which is isomorphic to  $Q$ ,  $d$  corresponds to the original  $p$ -adic metric which was defined on  $Q \times Q$  in the previous chapter.

Theorem 1.  $Q$  is complete with respect to the metric  $d$  of the preceding definition.

Proof: Let  $\{\alpha_n\}$  be a Cauchy sequence in  $Q_p$ . If  $\epsilon > 0$  there exists  $N$  such that  $d(\alpha_m, \alpha_n) < \epsilon$  for every  $m, n > N$ . Let  $\alpha_m$  be represented by  $\{x_i^{(m)}\}$  and  $\alpha_n$  be represented by  $\{x_i^{(n)}\}$  where the superscripts,  $(m)$  and  $(n)$ , are simply identification labels rather than exponents.

Since  $\{x_i^{(m)}\}$  is a Cauchy sequence in  $Q$  for every  $m$ , there exists an integer  $j_n$  such that for every  $i > j_n$ ,

$$\phi_p(x_i^{(m)} - x_{j_n}^{(m)}) < \frac{1}{n}. \text{ Let } \gamma \text{ denote the sequence } \{x_{j_1}^{(1)}, x_{j_2}^{(2)}, \dots, x_{j_n}^{(n)}, \dots\} \text{ and let } \overline{\{x_{j_n}^{(n)}\}} \text{ be the}$$

equivalence class determined by the constant sequence

$$\{x_{j_n}^{(n)}, x_{j_n}^{(n)}, \dots, x_{j_n}^{(n)}, \dots\}. \text{ Then}$$

$$d\left(\alpha_n, \overline{\{x_{j_n}^{(n)}\}}\right) = \lim_{j \rightarrow \infty} \phi_p(x_j^{(n)} - x_{j_n}^{(n)}) < \frac{1}{n}.$$

Hence

$$\begin{aligned} \phi_p(x_{j_n}^{(n)} - x_{j_m}^{(m)}) &= d\left(\overline{\{x_{j_n}^{(n)}\}}, \overline{\{x_{j_m}^{(m)}\}}\right) \\ &\leq d\left(\overline{\{x_{j_n}^{(n)}\}}, \alpha_n\right) + d(\alpha_n, \alpha_m) + d\left(\alpha_m, \overline{\{x_{j_m}^{(m)}\}}\right) \\ &< \frac{1}{n} + d(\alpha_n, \alpha_m) + \frac{1}{m} \end{aligned}$$

Therefore, given  $\epsilon > 0$ , by requiring that  $N$  be large enough

$$\text{so that for every } n, m > N, \frac{1}{n} < \frac{\epsilon}{3}, d(\alpha_m, \alpha_n) < \frac{\epsilon}{3}$$

and  $\frac{1}{m} < \frac{\epsilon}{3}$ , one has

$$\phi_p(x_{j_n}^{(n)} - x_{j_m}^{(m)}) < \epsilon.$$

Thus  $\gamma$  is a Cauchy sequence in  $Q$ . The equivalence class containing  $\gamma$  will be denoted by  $\bar{\gamma}$ .

If  $\epsilon > 0$ , then, since  $\gamma$  is a Cauchy sequence, there exists  $N$  such that for every  $n > N$ ,  $\phi_p(x_{j_n}^{(n)} - x_{j_N}^{(N)}) < \frac{\epsilon}{2}$ . Thus  $d(\bar{\gamma}, \overline{\{x_{j_N}^{(N)}\}}) = \lim_{m \rightarrow \infty} \phi_p(x_{j_m}^{(m)} - x_{j_N}^{(N)}) < \frac{\epsilon}{2}$  and, therefore,

$$\begin{aligned} d(\bar{\gamma}, \alpha_n) &\leq d(\bar{\gamma}, \overline{\{x_{j_n}^{(n)}\}}) + d(\overline{\{x_{j_n}^{(n)}\}}, \alpha_n) \\ &\leq d(\bar{\gamma}, \overline{\{x_{j_n}^{(n)}\}}) + \frac{1}{n} \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$

whenever  $n > \max \left[ N, \frac{2}{\epsilon} \right]$ . Consequently,  $\bar{\gamma} = \lim_{n \rightarrow \infty} \alpha_n$ , and  $Q_p$  is complete.

Since the number of primes is infinite, one may quite naturally ask if this implies that the number of completions of the rational field is infinite. The theorem which follows gives an affirmative answer.

**Theorem 2.** If  $p$  and  $q$  are distinct primes, then  $Q_p$  is not isomorphic to  $Q_q$ .

**Proof:** If  $Q_p$  were isomorphic to  $Q_q$  their additive identities would have to correspond. The additive identity of  $Q_p$  may be represented by  $\{x_n\}$  where  $x_n = p^n$ ,

but if  $q \neq p$  then  $\phi_q(x_n - 0) = \phi_q(p^n) = 1$ . Hence  $\{x_n\}$  is not a representative of the additive identity of  $Q_p$ , and, consequently,  $Q_p$  is not isomorphic to  $Q_q$ .

Using exactly the same type of argument as above, one obtains

Theorem 3. The real field is not isomorphic to  $Q_p$  for any prime,  $p$ .

In the previous chapter it was established that every  $p$ -adic number could be represented as an infinite series,  $\sum_{i=m}^{\infty} a_i p^i$ , just as every real number may be represented as a convergent series of powers of 10. The analogy extends much farther than this, however, as evidenced by the following theorem from Bachman (1).

Theorem 4. A  $p$ -adic number,  $\alpha$ , is a rational number if and only if its canonical expansion is periodic.

Proof: Suppose the canonical expansion of  $\alpha$  is periodic; then  $\alpha$  may be written as

$$\begin{aligned} \alpha &= a_m p^m + a_{m+1} p^{m+1} + \dots + a_{m+k} p^{m+k} \\ &\quad + b_1 p^{m+k+1} + b_2 p^{m+k+2} + \dots + b_j p^{m+k+j} \\ &\quad + b_1 p^{m+k+j+1} + \dots + b_j p^{m+k+2j} \\ &\quad + \dots \\ &= p^m (a_m + a_{m+1} p + \dots + a_{m+k} p^k) \\ &\quad + p^{m+k+1} (b_1 + b_2 p + \dots + b_j p^{j-1}) \\ &\quad + p^{m+k+j+1} (b_1 + b_2 p + \dots + b_j p^{j-1}) \end{aligned}$$

$$+ \dots$$

$$= p^m A + p^{m+k+1} B (1 + p^j + p^{2j} + \dots)$$

where

$$A = a_m + a_{m+1} p + \dots + a_{m+k} p^k$$

and

$$B = b_1 + b_2 p + \dots + b_j p^{j-1}.$$

Consequently,

$$\alpha = p^m A + p^{m+k+1} B \frac{1}{1-p^j}.$$

Thus  $\alpha$  is the sum of two rational numbers and is therefore rational.

Conversely, if  $\alpha$  is a non-zero rational number, one may write  $\alpha = p^n \beta$  where  $\beta = \frac{a}{b}$  with  $a$  and  $b$  integers such that  $p \nmid a$  and  $p \nmid b$ . There then exists, by the Euler-Fermat theorem, an integer  $j$  such that  $p^j \equiv 1 \pmod{b}$ . Thus

$$\beta = \frac{a}{b} = \frac{a(p^j - 1)}{b(p^j - 1)}$$

where  $b \mid (p^j - 1)$ . Hence

$$\alpha = p^n \beta = p^n \frac{t}{p^j - 1}$$

where  $t$  is an integer. Furthermore  $t \geq 0$  if and only if  $\alpha \geq 0$ .

Let an integer,  $k$ , be chosen such that  $0 \leq t < p^{k+1}$  if  $\alpha \geq 0$  or  $-p^{k+1} \leq t < 0$  if  $\alpha < 0$ . Since  $(p^{k+1}, p^j - 1) = 1$ , there exists by Theorem 9 of Chapter II, a unique solution  $(\text{mod } p^j - 1)$  of



$$p^{k+1} \cdot x \equiv -t \pmod{(p^j-1)}.$$

Choose a solution, B, such that

$$0 \leq B \leq p^j - 2 \text{ if } \alpha \geq 0 \text{ and } 1 \leq B \leq p^j - 1 \text{ if } \alpha < 0.$$

Since  $p^{k+1} B \equiv -t \pmod{(p^j-1)}$ , there exists an integer A such that  $t = A(p^j-1) - Bp^{k+1}$ . Furthermore,  $0 \leq A < p^{k+1}$  whether

$\alpha \geq 0$  or  $\alpha < 0$ , for if  $\alpha \geq 0$  then

$$0 \leq A(p^j-1) - Bp^{k+1} < p^{k+1}$$

and

$$0 \leq B \leq p^j - 2.$$

Whence

$$A(p^j-1) \geq A(p^j-1) - Bp^{k+1} \geq 0$$

And it follows that  $A \geq 0$ . Also

$$A(p^j-1) - (p^j-2)p^{k+1} < p^{k+1}$$

$$A(p^j-1) < [(p^j-2)+1] p^{k+1}$$

$$A(p^j-1) < (p^j-1)p^{k+1}$$

and hence  $A < p^{k+1}$ .

In a similar manner one can establish that if  $\alpha < 0$ , it is still true that  $0 \leq A < p^{k+1}$ . Consequently,

$$\alpha = p^n \frac{A(p^j-1) - Bp^{k+1}}{p^j-1}$$

where  $0 \leq A < p^{k+1}$ ,  $0 \leq B \leq p^j - 1$ . Thus

$$\alpha = p^n A + p^{n+k+1} B \cdot \frac{1}{1-p^j}$$

where  $A = \sum_{i=0}^r a_i p^i$  and  $B = \sum_{i=0}^{j-1} b_i p^i$ .

$$\text{Hence } \alpha = \sum_{i=0}^r a_i p^i + p^{n+k+1} \sum_{i=0}^{j-1} b_i p^i \left( \sum_{m=0}^{\infty} p^{mj} \right)$$

$$\begin{aligned} \text{or } \alpha &= a_0 p^n + a_1 p^{n+1} + \dots + a_r p^{n+r} \\ &+ p^{n+k+1} (b_0 + b_1 p + \dots + b_{j-1} p^{j-1}) \\ &+ p^{n+k+j+1} (b_0 + b_1 p + \dots + b_{j-1} p^{j-1}) \\ &+ p^{n+k+2j+1} (b_0 + b_1 p + \dots + b_{j-1} p^{j-1}) \\ &+ \dots \end{aligned}$$

$$\begin{aligned} \alpha &= a_0 p^n + a_1 p^{n+1} + \dots + a_r p^{n+r} \\ &+ b_0 p^{n+k+1} + b_1 p^{n+k+2} + \dots + b_{j-1} p^{n+k+j} \\ &+ b_0 p^{n+k+j+1} + b_1 p^{n+k+j+2} + \dots + b_{j-1} p^{n+k+2j} \\ &+ \dots \end{aligned}$$

Consequently, if  $\alpha$  is rational, its canonical  $p$ -adic representation is periodic.

The student of analysis learns early that if a series of real numbers,  $\sum_{n=1}^{\infty} \frac{U_n}{n}$ , converges then  $U_n \rightarrow 0$  as  $n \rightarrow \infty$ . He generally learns, also, by studying the harmonic series  $\sum_{n=1}^{\infty} \frac{1}{n}$  that the converse is not necessarily true. In this regard the  $p$ -adic numbers furnish a very interesting contrast.

**Theorem 4.** A  $p$ -adic series  $\sum_{n=1}^{\infty} U_n$  converges if and only if  $U_n \rightarrow 0$  as  $n \rightarrow \infty$ ,

**Proof:** Suppose first that  $\sum_{n=1}^{\infty} U_n$  converges. Then there exists  $N_k$  such that for every  $m > N_k$  and for all  $r \geq 0$ ,

$$\phi_p \left( \sum_{n=m}^{m+r} U_n \right) < \frac{1}{k}.$$

Thus if  $r=0$ ,  $\phi_p(U_m) < \frac{1}{k}$  for every  $m > N_k$ . Hence  $U_n \rightarrow 0$  in the  $p$ -adic metric whenever  $\sum_{n=1}^{\infty} U_n$  converges.

On the other hand if  $U_n \rightarrow 0$  in the  $p$ -adic metric, then for any arbitrary  $\epsilon > 0$  there exists  $N$  such that for every

$m > N$ ,  $\phi_p(U_m) < \epsilon$ . Consequently, for every  $r \geq 0$ ,

$$\phi_p \left( \sum_{n=m}^{m+r} U_n \right) \leq \text{Max} \left[ \phi_p(U_m), \phi_p(U_{m+1}), \dots, \phi_p(U_{m+r}) \right] < \epsilon$$

and  $\sum_{n=1}^{\infty} U_n$  converges by the Cauchy criterion for convergence in metric spaces.

#### Summary and Conclusions

In this study the  $p$ -adic numbers have been investigated as distinct entities which were worthy of study in their own right. They were developed as a completion of the field of rational numbers, and it was established that there was no other completion excepting the field of real numbers. This study has not investigated any of the applications of  $p$ -adic numbers. Any study of their applications, however, is likely to lead directly to their relationship to the theory of numbers and, in particular, to the theory of congruences. Borevich and Shafarevich (2) perhaps summarize the primary applications of the  $p$ -adic numbers

when they assert that in questions of divisibility the p-adic numbers are just as important as are the real numbers in questions of size.

During the course of this study, many interesting avenues for further investigation have arisen. There have appeared questions concerning the geometry of p-adic numbers, possible topologies of the p-adic numbers, algebra and analysis in the p-adic fields, and possible orderings of the p-adic numbers.

In regard to the latter question, Cohen and Ehrlich (3) prove that: "Any complete Archimedean ordered field is isomorphic to the ordered field of real numbers." This, of course, rules out an Archimedean ordering of the p-adic fields.

Mahler (9) in 1940 published a rather extensive article concerning a geometrical representation of p-adic numbers. Under his representation scheme a p-adic integer would correspond to a certain infinite set of points  $\{z_n\}$  in the upper half of the complex plane. To the reader who is interested in the geometry of numbers, Mahler's article might serve as a foundation for very fruitful work.

## BIBLIOGRAPHY

- (1) Bachman, George. Introduction to p-Adic Numbers and Valuation Theory. New York: Academic Press, 1964.
- (2) Borevich, Z. I., and I. R. Shafarevich. Number Theory. New York: Academic Press, 1966.
- (3) Cohen, Leon W., and Gertrude Ehrlich. The Structure of the Real Number System. Princeton: Van Nostrand, 1963.
- (4) Dynkin, E. B., and V. A. Uspenskii. Problems in the Theory of Numbers. Boston: D. C. Heath, 1963.
- (5) Hensel, Kurt. Theorie der Algebraischen Zahlen. Berlin: Teubner, 1908.
- (6) Jones, Burton W. The Arithmetic Theory of Quadratic Forms. Buffalo: The Mathematical Association of America, 1950.
- (7) Long, Calvin T. Elementary Introduction to Number Theory. Boston: D. C. Heath, 1965.
- (8) MacDuffee, C. C. "The p-Adic Numbers of Hensel." The American Mathematical Monthly. Vol. 45 (1938) 500-508.
- (9) Mahler, Kurt. "On a Geometrical Representation of p-Adic Numbers." Annals of Mathematics. Vol. 41. (1940) 8-56.
- (10) Mahler, Kurt. Lectures on Diophantine Approximations. Notre Dame: University of Notre Dame, 1961.
- (11) Niven, Ivan, and Herbert S. Zuckerman. An Introduction to the Theory of Numbers. 2nd ed. New York: Wiley, 1966.

- (12) Thurston, H. A. The Number System. New York: Interscience, 1956.
- (13) Van Der Waerden, B. L. Modern Algebra. New York: Frederick Ungar, 1953.

## VITA

Richard Preston Savage

Candidate for the Degree of

Doctor of Education

**Thesis:** P-ADIC NUMBERS

**Major Field:** Higher Education

**Biographical:**

**Personal Data:** Born near Palmer, Tennessee, February 17, 1930, the son of Jesse L. and Pearl Stockwell Savage.

**Education:** Attended Tatesville grade school in Palmer, Tennessee; graduated from Baxter Seminary, Baxter Tennessee in 1947; attended Tennessee Polytechnic Institute, 1947-1950; received the Bachelor of Science degree from the University of Chattanooga, with a major in Secondary Education, in June, 1955; received the Master of Science degree from the Oklahoma State University, with a major in Natural Science, in May, 1957; attended the University of Tennessee, 1957-1959; completed requirements for the Doctor of Education degree in May, 1968.

**Professional Experience:** Served in the United States Army, 1951-1953; taught in the public schools of Sequatchie County, Tennessee in 1950, 1953, 1954, and 1955-1956; taught mathematics at the University of Tennessee, 1957-1959; taught mathematics at Tennessee Wesleyan College, 1959-1960; served as Associate Mathematician with Union Carbide Nuclear Company, Oak Ridge, Tennessee, 1960-1962; has been teaching mathematics at Tennessee Technological University since 1962.