

PRIMES IN ARITHMETIC PROGRESSIONS

By

MELVIN ROBERT WOODARD

Bachelor of Science
Mansfield State College
Mansfield, Pennsylvania
1958

Master of Arts
University of Illinois
Urbana, Illinois
1962

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
July, 1966

OKLAHOMA
STATE UNIVERSITY
LIBRARY

JAN 27 1967

PRIMES IN ARITHMETIC PROGRESSIONS

W Ware Marsden

Thesis Adviser

Jeannie Agnew

Vernon Trope

Nielson E Berg

JMB

Dean of the Graduate College

ACKNOWLEDGMENTS

I am deeply indebted to Dr. Jeanne Agnew for the guidance and assistance which she provided during the preparation of this thesis. I also wish to thank Dr. W. Ware Marsden for serving as committee chairman; Drs. Vernon Troxel and Milton Berg for serving on my advisory committee; and Dr. L. Wayne Johnson, for his wise counsel.

To my wife, Lenora, and my children, Mary Kay and Mark, I express gratitude for the sacrifices which they made while assisting in the completion of my program of study.

TABLE OF CONTENTS

Chapter	Page
I. INTRODUCTION AND STATEMENT OF THE PROBLEM	1
Introduction	1
Statement of the Problem	3
Procedure	4
Scope and Limitations	4
Expected Outcomes	5
II. ELEMENTARY INTRODUCTION TO DIRICHLET'S THEOREM	6
III. ARITHMETIC PROGRESSIONS WITH ALL TERMS PRIME	13
IV. GENERALIZATIONS ON PAP'S	25
Prime Twins	25
Prime Quadruplets	30
Conjecture H	34
V. SPECIAL CASES OF DIRICHLET'S THEOREM	43
VI. DIRICHLET'S THEOREM	71
Characters	72
L-Functions	80
VII. SUMMARY AND EDUCATIONAL IMPLICATIONS	86
Summary	86
Educational Implications	87
A SELECTED BIBLIOGRAPHY	88

LIST OF TABLES

Table	Page
I. Natural Numbers in Columns of 10	7
II. Natural Numbers in Columns of 12	9
III. Natural Numbers in Columns of 4	13
IV. Arithmetic Progressions of the Form 3, $3 + 4k$, $3 + 8k$.	15
V. Natural Numbers in Columns of 6	17
VI. Approximations of R_d	27
VII. Rational Approximations of R_d	29
VIII. Values of R_d , Observed and Theoretical	30

CHAPTER I

INTRODUCTION AND STATEMENT OF THE PROBLEM

Introduction

The positive integers $1, 2, 3, \dots$ are called the natural numbers. These numbers form the basis for the study of the theory of numbers. The name, theory of numbers, might suggest that it is a kind of general theory concerning the notion of number and its generalizations which, starting from the integers, introduces successively, rational, real, and complex numbers, and perhaps some other kinds of numbers, and builds up a theory of operations on these numbers. This, however, is not the case. Elementary theory of numbers is concerned primarily with the properties of the integers, while the theory of operations on them is a part of higher arithmetic, or algebra.

From earliest times man has shown curiosity about the natural numbers. This is particularly true of the ancient Chinese and Greeks. It was not until the seventeenth century, however, that a serious study of number theory was made. Much of the work was done by the French mathematician Pierre de Fermat (1601-1665). Because of his leadership in this area he is often referred to as the founder of the theory of numbers. Another leader in the field was Carl Friedrich Gauss, who was not only a mathematician, but also a physicist and astronomer. He once indicated his partiality for mathematics in general, and for

the theory of numbers in particular, by stating that "mathematics is the queen of the sciences and the theory of numbers is the queen of mathematics." G.H. Hardy [8]¹, a twentieth century mathematician, made the following statement concerning the theory of numbers:

The elementary theory of numbers should be one of the best subjects for early mathematical instruction. It demands very little previous knowledge, its subject matter is tangible, and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity.

The study of the theory of numbers does not employ integers exclusively, however. Many properties of integers have been discovered with the aid of irrational or complex numbers and many theorems about integers can be proved in a much simpler way if one makes use not only of irrational or complex numbers, but also of calculus and theory of functions. The part of number theory which makes extensive use of various parts of analysis is called the analytic theory of numbers, to be distinguished from the elementary theory of numbers, which does not use the notion of limit.

Because the concept of natural number is so simple, one might think that there is not much left to discover in this area. This is not the case, since as some problems are being solved, more questions are being asked. As an illustration of the progress that the theory of numbers has made in the last fifteen years, two examples can be cited. In 1950, the largest prime number known was $2^{127} - 1$, which has 39 digits, compared with the largest prime known today, $2^{11213} - 1$ of 8376

¹Numbers in brackets refer to references in bibliography.

digits. In 1950 only 12 perfect numbers were known; as of this date 23 have been found. Many other discoveries and advances have been and are being made in this fascinating subject.

Statement of the Problem

Many of the ideas of elementary number theory provide motivational material for secondary school students. Some of the material forms a basis for many ideas that are presented in the so-called "modern mathematics" of elementary school. Because of its importance, number theory will probably become one of the required courses for all secondary school teachers and perhaps even elementary school teachers. The Course Guide for the Training of Teachers of Elementary Mathematics [16] written in July, 1964 by the Committee on Undergraduate Program in Mathematics (CUPM) recommends that number theory be taught as a part of a two course sequence devoted to the structure of the real number system and its subsystems. A similar guide [15] for the training of secondary school teachers recommends a full course in number theory for all future teachers of high school mathematics. It is therefore important that number theory be emphasized in the teacher training institutions.

The purpose of this paper is not to write a number theory text, but to take one small part of number theory, that dealing with primes in arithmetic progressions, and bring together in one volume the material that has been written on the subject. It is expected that many high school students, as well as their teachers, will be able to comprehend much of the material of this paper.

Procedure

A survey and analysis of the published results concerning primes in arithmetic progressions was made. The Mathematical Review, bibliographies of texts, bibliographies of published papers, and bibliographies of unpublished theses served as primary tools for locating source papers. Some of the results given were found in journals written in foreign languages and the results have not appeared before in English. The material was analyzed and presented in an expository manner. The material was also organized in an increasing sequence of difficulty. Chapter II provides an introduction to Dirichlet's famous theorem and is, along with Chapter III and part of Chapter IV, directed to secondary school students. The remaining part of Chapter IV and Chapter V presupposes a knowledge of elementary number theory, while Chapter VI is for those students possessing the mathematical maturity of a beginning graduate student.

Scope and Limitations

The published material concerning primes in arithmetic progressions is quite extensive, therefore this paper is limited to those topics which are applicable to the various audiences mentioned above.

This paper is based upon two types of progressions, finite and infinite, and their applications. A finite arithmetic progression is a sequence of the form $ak + b$ ($k = 0, 1, 2, \dots, n$), where b is the first term, a is the common difference and $an + b$ is the last term. An infinite arithmetic progression is a sequence of the form $ak + b$ ($k = 0, 1, 2, 3, \dots$). In the former, progressions in which each term is prime will

be investigated. In the latter, the number of primes in the progression will be the focus of interest.

Expected Outcomes

It is expected that as a result of reading this paper an individual will become aware of the simplicity of some of the ideas of elementary number theory. It is also expected that high school teachers will find material that can be used as enrichment in high school algebra, and that students studying elementary number theory will be able to understand how the basic theorems of the course can be used to prove theorems about primes in arithmetic progressions. Finally, it is hoped that this material will stimulate the reader's interest in mathematics.

CHAPTER II

ELEMENTARY INTRODUCTION TO DIRICHLET'S THEOREM

Although the reader is probably familiar with the notions of elementary number theory, in this chapter such an assumption will not be made. The basic definitions, notations, and operations that are needed will therefore be given.

Probably the most basic aspect of the natural numbers is the attribute of being prime or composite. Before defining this, the concept of a divisor is needed. This concept is associated with the integers, which include the natural numbers, zero, and the negatives of the natural numbers.

Definition 2.1. An integer d is said to divide an integer a if there is an integer c such that $a = dc$. In this case d is called a divisor of a and a is called a multiple of d . If d is a divisor of a we write $d|a$.

Definition 2.2. If d is a divisor of a and d is a divisor of b , then d is called a common divisor of a and b .

Definition 2.3. If p is an integer greater than 1 whose only positive divisors are 1 and p itself, then p is called a prime. If p is greater than 1 and is not prime, then it is called composite.

The problems with which this paper is concerned can be under-

stood by examining a table of the natural numbers written in a form similar to that of Table I. Upon examining the table it is evident that the first row consists of all numbers whose units digit is 1; the next row contains numbers with 2 as the units digit, etc.. One natural question is: How many prime numbers are there in any given row? Since Euclid proved that there is an infinite number of prime numbers, at least one of the rows must contain an infinite number of primes. For suppose each row contained less than k primes; since there are 10 rows there would be less than $10k$ primes, contradicting the fact that there is an infinite number of primes. Which row, or rows, then contain an infinite number of primes?

TABLE I
NATURAL NUMBERS IN COLUMNS OF 10

1	<u>11</u>	21	<u>31</u>	<u>41</u>	51	<u>61</u>	<u>71</u>	81	91	<u>101</u>	111	121 ...
<u>2</u>	12	22	32	42	52	62	72	82	92	102	112	122 ...
<u>3</u>	<u>13</u>	<u>23</u>	33	<u>43</u>	<u>53</u>	63	<u>73</u>	<u>83</u>	93	<u>103</u>	<u>113</u>	123 ...
4	14	24	34	44	54	64	74	84	94	104	114	124 ...
<u>5</u>	15	25	35	45	55	65	75	85	95	105	115	125 ...
6	16	26	36	46	56	66	76	86	96	106	116	126 ...
<u>7</u>	<u>17</u>	27	<u>37</u>	<u>47</u>	57	<u>67</u>	77	87	<u>97</u>	<u>107</u>	117	<u>127</u> ...
8	18	28	38	48	58	68	78	88	98	108	118	128 ...
9	<u>19</u>	<u>29</u>	39	49	<u>59</u>	69	<u>79</u>	<u>89</u>	99	<u>109</u>	119	129 ...
10	20	30	40	50	60	70	80	90	100	110	120	130 ...

The first row contains more than one prime; 11, 31, 41, and 61 are prime and there are others. There seems to be many primes in the

first row. The second row contains numbers divisible by 2. All numbers in this row, except 2, have at least three divisors, 1, 2, and the number itself, and so the only prime in this row is 2. The third row contains the primes 3, 13, and 23, and hence more than one prime. The fourth row is even less interesting than the second to those seeking prime numbers; the second row contains one prime, the fourth has none. The fifth row has the prime number 5 but all other entries in this row are divisible by 5 and therefore are not prime. The sixth row contains no primes since all numbers in this row are divisible by 2 and greater than 2. The seventh row has primes 7, 17, 37, and others. Rows eight and ten, like the sixth, are void of primes, while the ninth row contains the primes 19, 29, 59, and more.

The question concerning which rows have an infinite number of primes has been partially answered. Since rows 2, 4, 5, 6, 8, and 10 contain at most one prime, all primes greater than 10 must appear in rows 1, 3, 7, and 9; that is, at least one of these rows contains an infinite number of primes. The immediate questions are: how many, and which ones, have the desired property? These questions were answered only 130 years ago in a famous paper by P. L. Dirichlet (1805-1859). He proved that each of the rows 1, 3, 7, and 9 contains an infinite number of primes.

The theorem which he proved is much more general than the one discussed here. To make the meaning of his theorem clearer one might write the sequence of natural numbers in a form similar to that of Table I, but this time in columns of 12. Again the question is posed. Which rows contain primes and which rows contain many primes? As

TABLE II
NATURAL NUMBERS IN COLUMNS OF 12

1	<u>13</u>	25	<u>37</u>	49	<u>61</u>	<u>73</u>	85	<u>97</u>	<u>109</u>	121	133
<u>2</u>	14	26	38	50	62	74	86	98	110	122	134 ...
<u>3</u>	15	27	39	51	63	75	87	99	111	123	135 ...
4	16	28	40	52	64	76	88	100	112	124	136 ...
<u>5</u>	<u>17</u>	<u>29</u>	<u>41</u>	<u>53</u>	65	77	<u>89</u>	<u>101</u>	<u>113</u>	125	<u>137</u> ...
6	18	30	42	54	66	78	90	102	114	126	138 ...
<u>7</u>	<u>19</u>	<u>31</u>	<u>43</u>	55	<u>67</u>	<u>79</u>	91	<u>103</u>	115	<u>127</u>	<u>139</u> ...
8	20	32	44	56	68	80	92	104	116	128	140 ...
9	21	33	45	57	69	81	93	105	117	129	141 ...
10	22	34	46	58	70	82	94	106	118	130	142 ...
<u>11</u>	<u>23</u>	35	<u>47</u>	<u>59</u>	<u>71</u>	<u>83</u>	95	<u>107</u>	119	<u>131</u>	143 ...
12	24	36	48	60	72	84	96	108	120	132	144 ...

in Table I it appears that the first row contains many primes. The second row has 2 as its only prime. All elements in the third row can be characterized by the formula $12k + 3$ where k is the number of the column if the column on the left is called the 0 column. Since $12k + 3 = (4k + 1)3$ and $4k + 1$ is always a positive integer for $k = 0, 1, 2, \dots$ it follows that each element of the third row is divisible by 3, and so 3 is the only prime in this row. All numbers in the fourth row can be expressed in the form $12k + 4 = (3k + 1)4$ and so 4 divides all numbers in this row. Hence there can be no primes in row four. Similarly, numbers in the sixth, eighth, ninth, tenth, and twelfth rows can be written in the form $(1 + 2k)6$, $(2 + 3k)4$, $(3 + 4k)3$, $(5 + 6k)2$,

and $(1+k)12$, respectively. These rows, therefore, contain no primes.

There are at least six primes in each of the remaining rows as can be verified by Table II. It appears that there will be many more, however.

From a table such as this one it is possible to create general theorems about prime numbers. For instance, one might suspect that if a row contains many primes then the first number in that row must be prime. This is ruled out by checking row nine of Table I. It appears also that if the first two numbers of any row are prime then there are many primes in that row. The most important generalization that can be drawn from these examples concerns the first number in the row and its relationship to the common difference between adjacent columns. If these two numbers have a common divisor greater than 1 then this common divisor will divide all numbers in that row, and there can be no more than one prime in that row. In Table II the difference between adjacent columns is 12. The first number in the ninth row is 9. Both 12 and 9 are divisible by 3 and so 3 divides all elements in the ninth row. In the fifth row the first number is 5, and since the only common divisor of 5 and 12 is 1, it cannot be concluded that 5 divides all numbers in that row.

Challenge: Try to arrange the natural numbers in a form similar to that of Table I and obtain a row that contains exactly two primes.

Leonard Euler (1707-1783) was probably the first mathematician to make a conjecture publicly concerning the number of primes in a progression of the type mentioned above. He claimed, in 1775, that there

is an infinite number of primes in the progression $ak + 1$ ($k = 0, 1, 2, \dots$) where a is any natural number. Legendre (1752-1883) claimed a proof of the existence of an infinite number of primes in the progression $2ka + b$ ($k = 0, 1, 2, \dots$) if the only common divisor of $2a$ and b is 1. In his proof, however, he used a lemma that was later shown by Dupr  to be false. This paved the way for Dirichlet's famous theorem in 1837. Before stating this theorem two more definitions are needed.

Definition 2.4. A positive integer, d , is called the greatest common divisor of the integers a and b if d is a common divisor of a and b and is a multiple of every other common divisor. If d is the greatest common divisor of a and b we write $d = (a, b)$.

Definition 2.5. The natural numbers a and b are said to be relatively prime if and only if $(a, b) = 1$.

Dirichlet's Theorem. If a and b are relatively prime, then there exists an infinite number of primes in the progression $ak + b$ ($k = 0, 1, 2, 3, \dots$).

Euler's conjecture is therefore one special case of Dirichlet's Theorem since 1 and any other natural number are always relatively prime.

Because the proof of Dirichlet's Theorem is difficult, many mathematicians have proved and are proving special cases of it. Some involve fixed values for a and b , some only fixed b and still others only fixed a . Lucas gave a proof for the special case $5k + 2$ and $8k + 7$ in 1891; von Sterneck for $ak - 1$ in 1897; Carmichael for $p^n k - 1$, p an odd

prime and $2^n 3k - 1$, n a natural number, in 1913; and Marc Low and P. T. Bateman for $24k + b$ in 1965. Proofs of some of the special cases are given in Chapter V.

Another interesting problem that is suggested by Tables I and II concerns finding prime numbers in any given row that are equally spaced. For example, in row 1 of Table I it can be seen that 41, 71, and 101 are each prime and that there are two numbers in the row between each pair 41, 71, and 71, 101. In the language of elementary algebra one would say that the numbers 41, 71, and 101 form an arithmetic progression with common difference 30. In row seven another arithmetic progression with 3 prime terms can be found, namely, 67, 97, 127.

In Table II different arithmetic progressions with only prime terms can be found. In the first row the prime numbers 13, 37, 61, form an arithmetic progression with common difference 24. In row five the first 5 terms are all prime and form an arithmetic progression with common difference 12.

All numbers in Table I are of the form $10k + b$ where b is the first term of the row and k determines the column. The numbers in Table II are expressed as $12k + b$ where the k and b are as in Table I. By listing the natural numbers in other similar manners it is possible to discover other arithmetical progressions containing only prime terms. This and necessary conditions for the existence of certain arithmetical progressions is the subject of the next chapter.

CHAPTER III

ARITHMETIC PROGRESSIONS WITH ALL TERMS PRIME

Consider the natural numbers as they are arranged in Table III. Each of the rows is an infinite arithmetic progression with first term 1, 2, 3, or 4 and common difference 4. In the third row the numbers 3, 7, 11, form a finite arithmetic progression consisting only of prime numbers. The numbers 11, 15, 19, also form an arithmetic progression but 15 is not prime. Another arithmetic progression is 19, 27, 35, but in this case 19 is the only prime term.

TABLE III
NATURAL NUMBERS IN COLUMNS OF 4

1	<u>5</u>	9	<u>13</u>	<u>17</u>	21	25	<u>29</u>	33	<u>37</u>	<u>41</u> ...
<u>2</u>	6	10	14	18	22	26	30	34	38	42 ...
<u>3</u>	<u>7</u>	<u>11</u>	15	<u>19</u>	<u>23</u>	27	<u>31</u>	35	39	<u>43</u> ...
4	8	12	16	20	24	28	32	36	40	44 ...

Definition 3.1. A prime arithmetic progression (PAP) is an increasing arithmetic progression which contains only prime terms and which contains at least two distinct terms.

A PAP with two terms and common difference 2 is called a prime twin pair. A discussion of prime twin pairs is included in Chapter IV.

One PAP of three terms is 3, 7, 11. Notice that this PAP consists of the three terms of the third row of Table III. There are other PAP's in the third row of Table III, namely 3, 11, 19 and 19, 31, 43, but are there other PAP's in this row with a common difference 4? This question is answered by Theorem 3.1.

Theorem 3.1. The arithmetic progression 3, 7, 11, is the only PAP of three terms in the progression $4k + 3$ ($k = 0, 1, 2, \dots$).

Proof: Suppose there is another PAP of three consecutive terms in this progression. Let

$$c, c + 4, c + 8$$

represent the prime terms of the progression. If $c = 1$ or $c = 2$, then the progression is not a PAP. If $c = 3$, the progression 3, 7, 11, is generated. Therefore $c > 3$. Since every integer can be written in the form $3t$, $3t + 1$, or $3t + 2$, for some integer t , c can be written in one of these forms.

Now c is not of the form $3t$, for if it were it would be divisible by 3 and therefore not prime since $c > 3$. If $c = 3t + 1$ for some integer t , then

$$\begin{aligned} c + 8 &= (3t + 1) + 8 \\ &= 3t + 9 \\ &= 3(t + 3), \end{aligned}$$

and hence $c + 8$ is not prime. Therefore $c = 3t + 2$ for some integer t , and hence

$$\begin{aligned} c + 4 &= (3t + 2) + 4 \\ &= 3t + 6 \\ &= 3(t + 2), \end{aligned}$$

and in this case $c + 4$ is divisible by 3 and cannot be prime. Since there are only three possibilities and a contradiction results in each case, there can be no other PAP's of this form with common difference 4.

A proof similar to the one given would prove that 3, 11, 19, is the only PAP in the third row of Table III with common difference 8.

There are many PAP's in the third row with first term 3 containing exactly three terms. Two examples not already mentioned are 3, 31, 59, and 3, 67, 131.

Conjecture: There exists an infinite number of PAP's with three terms, first term 3, and each term of the form $4k + 3$.

This conjecture gains more meaning by writing the numbers of the form $4k + 3$ in a row. Above each number is placed a 3 and below each number the corresponding number $8k + 3$ is written. (See Table IV).

TABLE IV
ARITHMETIC PROGRESSIONS OF THE
FORM 3, $3 + 4k$, $3 + 8k$

	*	*			*		*			*			
3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	7	11	15	19	23	27	31	35	39	43	47	51	55
3	11	19	27	35	43	51	59	67	75	83	91	99	107
		*					*			*			
3	3	3	3	3	3	3	3	3 ...	3 ...	3 ...	3 ...	3 ...	3 ...
59	63	67	71	75	79	83	87 ...	107 ...	3+4k ...				
115	123	131	139	147	155	163	171 ...	211 ...	3+8k ...				

Each column in the table forms an arithmetic progression with difference $4k$. An asterisk is placed above each prime triple. Since $(3, 4) = 1$ and $(3, 8) = 1$, Dirichlet's Theorem proves that row two and row three each contain an infinite number of primes. To prove the conjecture one would have to prove that an infinite number of primes in row two are in a column with a prime of row three. Mathematicians have been unable to solve this seemingly simple problem.

Another question posed by Table III is this. Is there a PAP with first term 3 that has four terms? The answer is no.

Theorem 3.2. If 3 is the first term of a PAP then the PAP contains at most three terms.

Proof: Suppose a progression of four terms did exist. The terms could be represented by

$$3, 3 + d, 3 + 2d, 3 + 3d,$$

but $3 + 3d = 3(1 + d)$ is not prime since $(1 + d) > 0$.

Theorem 3.2 might lead one to believe that there would never be a PAP with four terms. The PAP 7, 19, 31, 43, shows that it is possible.

Another manner of expressing the natural numbers is shown in Table V. This table points out a fact about the primes that is used many times in elementary number theory. Rows two, three, four, and six each contain at most one prime, while rows one and five have many. The numbers in the first row are of the form $6k + 1$, while the numbers in row five are of the form $6k + 5$. This arrangement verifies that all prime numbers greater than 3 can be expressed in the form

$6t + 1$ or $6t + 5$ for some non-negative integer t . From this table one can find many PAP's with a common difference which is a multiple of 6.

TABLE V
NATURAL NUMBERS IN COLUMNS OF SIX

1	<u>7</u>	<u>13</u>	<u>19</u>	25	<u>31</u>	<u>37</u>	<u>43</u>	49	55	<u>61</u>	<u>67</u>	<u>73</u>	<u>79</u> ...
<u>2</u>	8	14	20	26	32	38	44	50	56	62	68	74	80...
<u>3</u>	9	15	21	27	33	39	45	51	57	63	69	75	81...
4	10	16	22	28	34	40	46	52	58	64	70	76	82...
<u>5</u>	<u>11</u>	<u>17</u>	<u>23</u>	<u>29</u>	35	<u>41</u>	<u>47</u>	<u>53</u>	<u>59</u>	65	<u>71</u>	77	<u>83</u> ...
6	12	18	24	30	36	42	48	54	60	66	72	78	84...

For example, 5, 11, 17, 23, 29; 17, 29, 41, 53; and 19, 31, 43; are three immediate ones. The results of the table also help establish the following theorem.

Theorem 3.3. Every PAP of three terms with first term greater than 3 has a common difference which is a multiple of 6.

Proof: Let b be the first term and d the common difference. Then

$$b, b + d, b + 2d,$$

represents the PAP. The proof will follow by showing that d is a multiple of 6. Since $b > 3$, b can be written in the form $6t + 1$ or $6t + 5$ for some non-negative integer t . Now d must be even, for if d were odd then $b + d$ would be even, greater than 2, and hence not prime. Also d is positive since a PAP is increasing. Since d is an integer, d can be represented in one of the following forms for some integer r .

$$6r, 6r + 1, 6r + 2, 6r + 3, 6r + 4, 6r + 5.$$

Since d must be even the second, fourth, and sixth possibilities are eliminated. That is, d is of the form $6r$, $6r + 2$ or $6r + 4$. The two cases for the b 's will be considered separately.

Case I. $b = 6t + 1$

$$\begin{aligned}\text{If } d = 6r + 2, \text{ for some } r, \text{ then } b + d &= (6t + 1) + (6r + 2) \\ &= 6r + 6t + 3 \\ &= 3(2r + 2t + 1),\end{aligned}$$

and thus $b + d$ is not prime.

$$\begin{aligned}\text{If } d = 6r + 4, \text{ for some } r, \text{ then } b + 2d &= (6t + 1) + 2(6r + 4) \\ &= 6t + 12r + 9 \\ &= 3(2t + 4r + 3),\end{aligned}$$

and so $b + 2d$ is not prime.

Case II. $b = 6t + 5$

$$\begin{aligned}\text{If } d = 6r + 2, \text{ for some } r, \text{ then } b + 2d &= (6t + 5) + 2(6r + 2) \\ &= 6t + 12r + 9 \\ &= 3(2t + 4r + 3),\end{aligned}$$

and as before, $b + 2d$ is not prime.

$$\begin{aligned}\text{If } d = 6r + 4, \text{ for some } r, \text{ then } b + d &= (6t + 5) + (6r + 4) \\ &= 6t + 6r + 9 \\ &= 3(2t + 2r + 3),\end{aligned}$$

and in this case $b + d$ is not prime.

Since five of the six possibilities for the representation of d have been ruled out, the only possibility left is for d to be of the form $6r$, that is, d is a multiple of 6, and the theorem is proved.

In checking for PAP's with first term greater than 3 it is only necessary to check those arithmetic progressions with common difference

6, 12, 18, 24, etc.. The theorem does not prove that every d of the form $6r$ will give a PAP, for if $b = 5$ and $d = 30$ then $b, b + d, b + 2d$, gives the progression 5, 35, 65, which is not a PAP.

Challenge: Consider the arithmetic progression $ak + b$ ($k = 0, 1, 2, \dots$). Let $b = 5$ and find which values of $a = 6, 12, 18, 24, \dots 66$, will generate a PAP.

Theorem 3.3 involved PAP's of three terms and first term greater than 3. Since a PAP of four terms contains a PAP of three terms it follows that a PAP of four terms with first term greater than 3 would also have a common difference which is a multiple of 6. Since Theorem 3.2 guarantees the nonexistence of PAP's of four terms and first term 3 the first term of a PAP with four terms must be greater than 3. Some of the progressions of three terms from the exercise above can be extended to PAP's of four terms. With $a = 6$ the PAP 5, 11, 17, 23, is obtained and when $a = 18$, the PAP 5, 23, 41, 59 is generated.

Challenge: Of the PAP's from the previous challenge, which ones can be extended to PAP's of four terms by taking $k = 3$?

Challenge: Find at least one PAP of four terms with first term 7; with first term 11; with first term 13; with first term 17.

The search for PAP's with five terms is more difficult yet. The progression with first term 11 and difference 60 is such a progression, in fact, more than the first five terms of this progression are prime. The following challenges will help the reader discover some facts about

PAP's.

Challenge: What is the first composite number in the progression $60k + 11$ ($k = 0, 1, 2, \dots$)?

Challenge: Find a PAP of five terms with first term 5; with first term 7; with first term 13.

Challenge: Find a PAP of six terms with first term 5.

There are other facts about PAP's that are helpful in locating certain ones. These facts are stated in the following four theorems.

Theorem 3.4. There does not exist a PAP of $b + 1$ terms and first term b .

Proof: Suppose such a progression did exist. Then the progression could be represented by

$$b, b + d, b + 2d, b + 3d, \dots, b + bd.$$

But $b + bd = b(1 + d)$ is not prime since $b \neq 1$ and $d > 0$.

It should be noted that Theorem 3.2 is a special case of this theorem.

The next theorem is similar to Theorem 3.3 since it involves information about the common divisor. It is interesting to note that as the number of terms in a PAP increases and the first term increases, the common difference must also increase.

Theorem 3.5. All PAP's with five terms and with first term greater than 5 have a common difference which is a multiple of 5.

Proof: Let $b, b + d, b + 2d, b + 3d, b + 4d$ represent the terms of the

progression. Every natural number can be written in one of the following forms: $5t$, $5t + 1$, $5t + 2$, $5t + 3$, $5t + 4$, for some non-negative integer t . Therefore, d can be represented in one of these forms. The proof follows by showing that if d is not of the form $5t$, then one of the terms of the progression is divisible by 5 and hence not prime, since all terms are greater than 5. Now all prime numbers greater than 5 have units digit 1, 3, 7, or 9 (see Table I, p. 7), and therefore b is of the form $10m + 1$, $10m + 3$, $10m + 7$, or $10m + 9$.

Case I. $b = 10m + 1$.

If $d = 5t + 1$, then $b + 4d = 10m + 1 + 4(5t + 1) = 5(2m + 4t + 1)$.

If $d = 5t + 2$, then $b + 2d = 10m + 1 + 2(5t + 2) = 5(2m + 2t + 1)$.

If $d = 5t + 3$, then $b + 3d = 10m + 1 + 3(5t + 3) = 5(2m + 3t + 2)$.

If $d = 5t + 4$, then $b + d = 10m + 1 + 5t + 4 = 5(2m + t + 1)$.

So if b is of the form $10m + 1$, then d must be of the form $5t$.

Case II. $b = 10m + 3$.

If $d = 5t + 1$, then $b + 2d = 10m + 3 + 2(5t + 1) = 5(2m + 2t + 1)$.

If $d = 5t + 2$, then $b + d = 10m + 3 + 5t + 2 = 5(2m + t + 1)$.

If $d = 5t + 3$, then $b + 4d = 10m + 3 + 4(5t + 3) = 5(2m + 4t + 3)$.

If $d = 5t + 4$, then $b + 3d = 10m + 3 + 3(5t + 4) = 5(2m + 3t + 3)$.

If b is of the form $10m + 3$, then d is of the form $5t$.

Case III. $b = 10m + 7$.

If $d = 5t + 1$, then $b + 3d = 10m + 7 + 3(5t + 1) = 5(2m + 3t + 2)$.

If $d = 5t + 2$, then $b + 4d = 10m + 7 + 4(5t + 2) = 5(2m + 4t + 3)$.

If $d = 5t + 3$, then $b + d = 10m + 7 + 5t + 3 = 5(2m + t + 2)$.

If $d = 5t + 4$, then $b + 2d = 10m + 7 + 2(5t + 4) = 5(2m + 2t + 3)$.

Hence if b is of the form $10m + 7$, then d is of the form $5t$.

Case IV. $b = 10m + 9$.

If $d = 5t + 1$, then $b + d = 10m + 9 + 5t + 1 = 5(2m + t + 2)$.

If $d = 5t + 2$, then $b + 3d = 10m + 9 + 3(5t + 2) = 5(2m + 3t + 3)$.

If $d = 5t + 3$, then $b + 2d = 10m + 9 + 2(5t + 3) = 5(2m + 2t + 3)$.

If $d = 5t + 4$, then $b + 4d = 10m + 9 + 4(5t + 4) = 5(2m + 4t + 5)$.

If b is of the form $10m + 9$, then again d is of the form $5t$. Since b is of one of the four forms listed it follows that d is of the form $5t$ and therefore is a multiple of 5.

A well-known theorem in elementary number theory states that if d is a multiple of a and d is a multiple of b , where $(a, b) = 1$, then d is also a multiple of the product of a and b . Since every PAP with first term greater than 5 satisfies the hypothesis of Theorem 3.3, the common difference d of Theorem 3.5 is both a multiple of 5 and a multiple of 6. Since $(5, 6) = 1$, the following theorem has been proved:

Theorem 3.6. All PAP's with five terms and with first term greater than 5 have a common difference which is a multiple of 30.

Challenge: With the aid of Theorem 3.6, find another PAP of five terms and first term 13; with first term 17.

PAP's with ten terms are known; for instance $210k + 199$ for $k = 0, 1, 2, \dots, 9$, is one example. The largest known PAP has thirteen terms. It is the progression $60060k + 4943$ for $k = 0, 1, 2, 3, \dots, 12$. It is not known whether or not there exists a PAP of a hundred terms. The following theorem, of which Theorems 3.3 and 3.5 are special cases, shows that if one does exist then the common difference would be a multiple of $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times \dots \times 97$, which has

more than 30 digits in its representation. With the aid of faster computers PAP's with more than thirteen terms will probably be found.

Theorem 3.7. [27] If n and d are natural numbers, $n > 1$, and if n terms of the arithmetical progression

$$b, b + d, b + 2d, b + 3d, \dots, b + (n - 1)d$$

are odd prime numbers, then the difference d is divisible by every prime number less than n .

Proof: Now $b \geq n$, because if $b < n$, then $b \leq n - 1$ and $b + bd = b(1 + d)$ would be a composite term of the progression.

Let p denote any prime number less than n . Divide each of the terms $b, b + d, b + 2d, \dots, b + (p - 1)d$ by p obtaining remainders $r_0, r_1, r_2, \dots, r_{p-1}$, respectively, where $0 < r_i < p$ since $b + id$ is prime for $0 \leq i \leq p - 1$. There are p remainders which can take on the values $1, 2, 3, \dots, p - 1$. So for some k and j where $0 \leq j < k \leq p - 1$, $r_k = r_j$. That is

$$b + kd = pQ_k + r_k$$

$$b + jd = pQ_j + r_j = pQ_j + r_k.$$

Hence,

$$\begin{aligned} pQ_k &= b + kd - r_k \\ &= b + kd - (b + jd - pQ_j) \\ &= kd - jd + pQ_j. \end{aligned}$$

Therefore p divides $kd - jd = (k - j)d$. But by the inequalities $0 < k - j \leq p - 1 < p$, it follows that p does not divide $k - j$ and so p must divide d . Since p was an arbitrary prime number less than b , the theorem follows.

Corollary: If a PAP consisting of n terms exists, then the common

difference d is divisible by the product of all prime numbers less than n , and is therefore greater than or equal to n .

Proof: The proof follows from the theorem and a generalization of the remarks preceding Theorem 3.6. That is, if d is a multiple of $a_1, a_2, a_3, \dots, a_k$ and the greatest common divisor of these numbers is 1, then d is a multiple of the product $a_1 \cdot a_2 \cdot a_3 \cdots a_k$.

CHAPTER IV

GENERALIZATIONS ON PAP'S

Prime Twins

As has already been noted, many of the problems of number theory are concerned with the number of prime numbers of a certain form. One method that one may use in attempting to solve these problems is to look at the difference between the primes. Since 2 and 3 are the only prime numbers with difference 1, one can proceed immediately to those primes with difference 2. In so doing one is really looking for PAP's with common difference 2. Theorem 3.3 guarantees that if the PAP has three terms and first term greater than 3 then the common difference is a multiple of 6, hence 3, 5, 7, must be the only progression of three or more terms and common difference 2. As was noted in Chapter III, progressions of two terms with difference 2 are called prime twin pairs. The natural question is: How many prime twin pairs are there? There are four pairs less than 25: 3, 5; 5, 7; 11, 13; and 17, 19. By checking a table of primes one can find all such pairs less than any desired number. There are 8 pairs less than 100; 7 between 100 and 200; none between 700 and 800 but 5 between 800 and 900. Neglecting noticeable irregularities there is a decrease in the frequency of prime twin pairs as one continues into the higher ranges of numbers. There are two pairs be-

tween 209200 and 209300 which are: 209201, 209203; and 209267, 209269. Thus there are prime twin pairs even in very high ranges, but their number does decrease. This is to be expected since the number of all primes in these ranges also decreases.

No one has been able to prove that there is an infinite number of prime twin pairs. D. H. and E. Lehmer [11] have found that there are 152,892 pairs less than 30 million. The greatest of the known pairs of twin primes is the pair 140737488353699, 140737488353701.

To generalize this idea of differences between primes consider the PAP's with exactly two terms. That is, consider all primes p such that another prime p' exists such that $p' = p + d$, where d is some fixed natural number. By so doing it is possible to note some interesting facts about the prime numbers. The situation is quite uninteresting unless d is even. The fact that other primes between p and p' might exist does not matter. The list of such primes with $d = 6$ such that the first prime does not exceed 100 is as follows: 5, 11; 7, 13; 11, 17; 13, 19; 17, 23; 23, 29; 31, 37; 37, 43; 41, 47; 47, 53; 53, 59; 61, 67; 67, 73; 73, 79; 83, 89; 97, 103. It is curious to note that in the range less than 100 there are more pairs of this kind than there are prime twin pairs. In fact, there are exactly twice as many. In the range less than 30 million there are 304867 primes followed by another prime of distance 6, or nearly twice as many as the number of prime twin pairs.

The numbers of these prime pairs have been obtained by Professor and Mrs. Lehmer with the appropriate use of computing apparatus; they computed up to 30 million the number of prime pairs $p, p + d$; where d takes on the values 2, 4, 6, 8, ..., 70.

In order to discuss the results it will be convenient to introduce some new notation. Let $\pi_d(x)$ represent the number of those primes p which satisfy the following conditions:

$$p \leq x, \quad p + d \text{ is a prime number.}$$

For instance, $\pi_2(100) = 8$ $\pi_2(30,000,000) = 152,892$

$$\pi_6(100) = 16 \quad \pi_6(30,000,000) = 304,867.$$

Then set $R_d = \pi_d(30,000,000)/\pi_2(30,000,000)$. For instance

$R_6 = 304,867/152,892 = 1.9940$. A small part of the material computed by the Lehmers is included in Table VI.

TABLE VI
APPROXIMATIONS OF R_d

d	R_d	d	R_d	d	R_d	d	R_d	d	R_d
2	1.0000	16	1.0001	30	2.6632	44	1.1097	58	1.0349
4	0.9979	18	1.9982	32	0.9970	46	1.0467	60	2.6632
6	1.9940	20	1.3311	34	1.9965	48	1.9965	62	1.0341
8	0.9996	22	1.1088	36	1.9997	50	1.3308	64	0.9999
10	1.3317	24	1.9976	38	1.0566	52	1.0892	66	2.2186
12	1.9985	26	1.0910	40	1.3330	54	1.9981	68	1.0663
14	1.1985	28	1.1974	42	2.3987	56	1.1957	70	1.5977

It has been pointed out that all primes greater than 5 have a units digit that is either 1, 3, 7, or 9. It is thought that there are as many of one kind as there are of another. Do the 35 kinds of prime numbers with which Table VI is associated occur with such regularity? If it were so then all ratios R_d of Table VI would be approximately 1. Remarkably enough, a few entries of Table VI are close to 1.

Perhaps, however, it is the case that the ratio $\pi_d(x)/\pi_2(x)$ may converge to some limit, not necessarily 1, as x approaches infinity and $R_d = \pi_d(30,000,000)/\pi_2(30,000,000)$ entered in Table VI may be an approximation of that limit.

The values for which R_d are close to 1 correspond to $d = 2, 4, 8, 16$ and 64 . These values are also the smallest values in the table. Are there other entries in the table as close to each other?

In trying to answer this question notice that the entries corresponding to $d = 6, 12, 24$, and 48 are approximately equal to each other, and so are those corresponding to $d = 10, 20$ and 40 or those corresponding to $d = 14, 28$, and 56 . In general, multiplication by 2 seems to leave R_d almost unchanged.

What about multiplication by 3? It approximately doubles the values of R_d in some cases, as from 2 to 6, 4 to 12, 8 to 24, 16 to 48, 10 to 30, 20 to 60, 14 to 42, and 22 to 66. Yet, in other cases this is not so, as from 6 to 18, 12 to 36, and 18 to 54. In these latter cases the multiplication by 3 leaves the values of R_d almost unchanged. It is hard to account for the regularities in some instances and irregularities in others. By checking more carefully one may discover that the values of R_d contained in Table VI come close to simple fractions. (See Table VII)

Table VII strongly suggests that R_d depends only upon the decomposition of d into prime factors. In other words, just the presence of a prime factor in, or its absence from, the decomposition seems to be relevant; for instance, to values d of the form $2^x 3^y$ with $x, y = 1, 2, 3, \dots$ there corresponds approximately the same value of R_d .

TABLE VII
RATIONAL APPROXIMATIONS OF R_d

	2	16	6	36	10	14	22	30	42	66	70
d	4	32	12	48	20	28	44	60			
	8	64	18	54	40	56					
			24		50						
R_d (approx)	1/1		2/1		4/3	6/5	10/9	8/3	12/5	20/9	8/5

Moreover, to each prime factor d there seems to correspond a factor of R_d ; to the unavoidable factor 2 of d , the trivial factor 1 of R_d ; to the prime factors 3, 5, 7 and 11 of d the factors $2/1$, $4/3$, $6/5$, and $10/9$ of R_d respectively.

Then, when d is a product of different primes or powers of primes, R_d seems to be the product of the corresponding factors.

The observations pointed out here point to the conjectural formula

$$\pi_d(x) \approx \pi_2(x) \prod_{p|d} \frac{(p-1)}{(p-2)}, \quad p > 2.$$

This formula is merely a conjecture which can be conceived by examining Table VI. In Table VIII the observed values of R_d taken from Table VI are compared with the corresponding conjectural limiting values.

To attempt an explanation of this seemingly simple yet amazing result is beyond the scope of this paper. The interested reader will be interested in Polya's attempt at an explanation. [17: 381-384]

Another interesting note concerning the number of primes and prime twins is the fact that the series $\sum_p \frac{1}{p}$, where the sum is over all

the primes, diverges, thus proving the existence of an infinite number of primes; however the series $\sum_{p+2=q} (\frac{1}{p} + \frac{1}{q})$ where p and q are prime, converges, and has been approximated to 3 decimal places by E. S. Selmer [22]. This does not imply that the number of twin primes is finite, however.

TABLE VIII
VALUES OF R_d , OBSERVED AND THEORETICAL

d	$R_d(\text{obs})$	$R_d(\text{theor})$	d	$R_d(\text{obs})$	$R_d(\text{theor})$	d	$R_d(\text{obs})$	$R_d(\text{theor})$
2	1.0000	1.0000	26	1.0910	1.0909	50	1.3308	1.3333
4	0.9979	1.0000	28	1.1974	1.2000	52	1.0892	1.0909
6	1.9940	2.0000	30	2.6632	2.6667	54	1.9981	2.0000
8	0.9996	1.0000	32	0.9970	1.0000	56	1.1957	1.2000
10	1.3317	1.3333	34	1.0645	1.0667	58	1.0349	1.0370
12	1.9985	2.0000	36	1.9997	2.0000	60	2.6632	2.6667
14	1.1985	1.2000	38	1.0566	1.0588	62	1.0341	1.0345
16	1.0001	1.0000	40	1.3330	1.3333	64	0.9999	1.0000
18	1.9982	2.0000	42	2.3987	2.4000	66	2.2186	2.2222
20	1.3311	1.3333	44	1.1097	1.1111	68	1.0663	1.0667
22	1.1088	1.1111	46	1.0467	1.0476	70	1.5977	1.6000
24	1.9976	2.0000	48	1.9965	2.0000			

Prime Quadruplets

Another generalization on the prime twin pair problem concerns primes in the finite sequence $p, p + 2, p + 6, p + 8$; for example 5, 7, 11, 13. Such sequences with all terms prime are called simply quadruplets. It is not known whether or not there exist infinitely many

such quadruplets. The first six consecutive quadruplets are obtained for $p = 5, 11, 101, 191, 821$ and 1481 . Hardy and Littlewood [9] found 165 quadruplets less than 100,000 and Sierpiński [25: 117] states that W. A. Golubew recently found 897 quadruplets less than 10 million.

Several known results concerning quadruplets are shown in the following theorems. The proofs are elementary in that only the very fundamental ideas of congruences are used.

Theorem 4.1. If $p, p + 2, p + 6, p + 8$ is a quadruplet and $p > 5$, then the four primes differ only in the units digit and these digits are 1, 3, 7, and 9 respectively.

Proof: Since $p > 5$, it is sufficient to show that p has units digit 1. This will follow by showing that if p has units digit other than 1 then one of the terms of the sequence is not prime. If p has units digit which is even then p is divisible by 2 and obviously not prime since $p > 5$. If p has a units digit which is 5, then p is divisible by 5 and not prime.

If p has units digit 3, 7, or 9, then $p + 2, p + 8, \text{ or } p + 6$ has units digit 5 respectively, and therefore is divisible by 5 and greater than 5, and hence not prime. The only possibility left is for p to have units digit 1.

The preceding theorem is extremely helpful to one using the "search" method to locate such quadruplets. The next theorem is not as helpful as far as locating quadruplets is concerned but the result is still quite amazing. The theorem is somewhat similar to Theorem 3.7 of the preceding chapter. The reason for the choice of the

number 210 is brought out in the proof.

Theorem 4.2. If $p \neq 5$ and $p, p + 2, p + 6$, and $p + 8$ are all prime, then dividing p by 210 leaves a remainder of 11, 101, or 191.

Proof: It is sufficient to show that at least one of the following holds:

$$p \equiv 11 \pmod{210}$$

$$p \equiv 101 \pmod{210}$$

$$p \equiv 191 \pmod{210}$$

Note first that 11, 101 and 191 are p 's that generate quadruplets and that 210 is the product of the first four primes. The proof will follow by showing that if $p \not\equiv 11 \pmod{210}$ and $p \not\equiv 101 \pmod{210}$ then $p \equiv 191 \pmod{210}$.

Now p must be of the form $6k - 1$, $k > 1$. This follows from the fact that all primes greater than 5 are of the form $6k - 1$ or $6k + 1$ (see Table V, Chapter III), and if p were of the form $6k + 1$, then $p + 2 = 6k + 3 = 3(2k + 1)$ would not be prime. Since p is odd it follows that

$$(1) \quad p \equiv 1 \pmod{2}.$$

Also since $p > 5$ it follows that either $p \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}$. But if $p \equiv 1 \pmod{3}$, then $p + 2 \equiv 1 + 2 \equiv 3 \equiv 0 \pmod{3}$, which implies that 3 divides $p + 2$. This is impossible since $p + 2$ is prime, hence it must be the case that

$$(2) \quad p \equiv 2 \pmod{3}.$$

Similarly p is congruent to 1, 2, 3, or 4 modulo 5.

If $p \equiv 2 \pmod{5}$, then $p + 8 \equiv 10 \equiv 0 \pmod{5}$ and $p + 8$ is not prime.

If $p \equiv 3 \pmod{5}$, then $p + 2 \equiv 5 \equiv 0 \pmod{5}$ and $p + 2$ is not prime.

If $p \equiv 4 \pmod{5}$, then $p + 6 \equiv 10 \equiv 0 \pmod{5}$ and $p + 6$ is not prime.

Hence it must be the case that

$$(3) \quad p \equiv 1 \equiv 191 \pmod{5}.$$

Also p is congruent to 1, 2, 3, 4, 5, or 6 modulo 7. If p is congruent to 1, 5, or 6 modulo 7, then $p + 6$, $p + 2$, or $p + 8$ is not prime respectively. Therefore either $p \equiv 2 \pmod{7}$, $p \equiv 3 \pmod{7}$ or $p \equiv 4 \pmod{7}$.

Now if $p \equiv 11 \pmod{210}$, then the following four conditions must all hold:

$$p \equiv 11 \equiv 1 \pmod{2}$$

$$p \equiv 11 \equiv 2 \pmod{3}$$

$$p \equiv 11 \equiv 1 \pmod{5}$$

$$p \equiv 11 \equiv 4 \pmod{7}$$

while if $p \equiv 101 \pmod{210}$ then in the same fashion the following four congruences are satisfied:

$$p \equiv 101 \equiv 1 \pmod{2}$$

$$p \equiv 101 \equiv 2 \pmod{3}$$

$$p \equiv 101 \equiv 1 \pmod{5}$$

$$p \equiv 101 \equiv 3 \pmod{7}.$$

Since it has been shown that $p \equiv 1 \pmod{2}$, $p \equiv 2 \pmod{3}$, and $p \equiv 1 \pmod{5}$ it follows that if $p \not\equiv 11 \pmod{210}$ and $p \not\equiv 101 \pmod{210}$, then $p \not\equiv 4 \pmod{7}$ and $p \not\equiv 3 \pmod{7}$. Therefore the following congruence holds.

$$(4) \quad p \equiv 2 \equiv 191 \pmod{7}.$$

Therefore by (1), (2), (3), and (4), it follows that

$$p \equiv 191 \pmod{2, 3, 5, \text{ and } 7},$$

hence:

$$p \equiv 191 \pmod{210},$$

and the theorem is proved.

Many other generalizations on prime twins could be made and more theorems proved. The triples of primes of the form p , $p + 2$, $p + 6$, or p , $p + 4$, $p + 6$ provide examples from which simple theorems can be proved. A different type of theorem concerning these sequences will be given in Chapter V.

Conjecture H

In the field of mathematics and number theory in particular, many conjectures are made. One such conjecture has already been discussed in this chapter. Sometimes the conjectures are proven and become theorems, while many times they remain unsolved or are proven false. Once a conjecture is made new challenges arise. Mathematicians attempt not only to prove or disprove the conjecture, but also try to find statements which are equivalent to, which follow from, or which imply the given statement. In so doing new mathematics is created.

In 1958, A. Schinzel [20: 188], a Polish mathematician, made a conjecture which has come to be known as Conjecture H. If proven, many of the unanswered questions of number theory would be solved including several that have been mentioned in this paper. The conjecture is based upon a certain class of polynomials with integral coefficients. It is known that there is no polynomial $f(x)$ having integral coefficients which gives a prime for each natural value of x . However, it is possible for a polynomial to give infinitely many prime values for natural values of x . The polynomial $f(x) = 2x + 1$ is one simple example, and it is conjectured that $f(x) = x^3 + 2$ is another.

There is a natural connection between prime numbers and polynomials which are irreducible over some set of coefficients. The polynomials with which Conjecture H is concerned are irreducible over the integers and can be illustrated as follows: let s denote a natural number and let $f_1(x), f_2(x), f_3(x) \dots, f_s(x)$ be polynomials with integral coefficients. Suppose there are infinitely many natural numbers x for which each of the polynomials $f_1(x), f_2(x) \dots, f_s(x)$ generate a prime. The coefficient a_{i_0} of the highest power of the variable x of $f_i(x)$ must be positive, because for large values of x the value of the polynomial at x has the same sign as a_{i_0} , hence $f_i(x)$, $i = 1, 2, 3, \dots, s$, can be arbitrarily large. Also $f_i(x)$ cannot be the product of two polynomials with integral coefficients otherwise for sufficiently large values of x , $f_i(x)$ would be composite. Therefore $f_i(x)$, $i = 1, 2, 3, \dots, s$, must be irreducible. This implies that there is no natural number $d > 1$ which divides the number $P(x) = f_1(x) \cdot f_2(x) \dots f_s(x)$, for any natural value of x . If such a number did exist it would be the divisor of s arbitrarily large prime numbers, which is impossible.

It therefore follows that if s is a natural number and $f_1(x), f_2(x), \dots, f_s(x)$ are polynomials whose coefficients are integers, and if for infinitely many natural numbers x , the numbers $f_1(x), f_2(x), \dots, f_s(x)$ are prime, then the polynomials must satisfy the following:

Condition S: Each of the polynomials $f_i(x)$, $i = 1, 2, 3, \dots, s$, is irreducible, its leading coefficient is positive, and there is no natural number $d > 1$ that is a divisor of each of the numbers $P(x) = f_1(x) \cdot f_2(x) \dots f_s(x)$, where x is an integer.

Conjecture H: [20: 188] If s is a natural number and if $f_1(x)$, $f_2(x), \dots, f_s(x)$ are polynomials with integral coefficients satisfying Condition S, then there exist infinitely many natural values of x for which each of the numbers $f_1(x), f_2(x), \dots, f_s(x)$ is a prime.

It can now be shown how some of the unanswered questions follow from Conjecture H. It must be noted, however, that the results follow from an unproven statement and by no means can be taken as theorems. The value of showing how statements follow from a conjecture is twofold. It demonstrates the interrelation of many other conjectures and it reformulates the problem so that an alternate approach to its proof might be taken. The first consequence that will be shown concerns the number of prime twin pairs.

Conjecture H implies that if a and b are natural numbers such that $(a, b) = 1 = (a, b(b + 2))$ then there exist infinitely many prime numbers p of the form $ak + b$, where k is a natural number, such that $p + 2$ is also a prime number. The result follows by letting $f_1(x) = ax + b$, $f_2(x) = ax + b + 2$, and $P(x) = f_1(x) \cdot f_2(x)$. Then $P(0) = b(b + 2)$, $P(1) = (a + b)(a + b + 2)$, and $P(-1) = (-a + b)(-a + b + 2)$. Then $P(1) + P(-1) = 2a^2 + 2b^2 + 4b = 2a^2 + 2b(b + 2)$.

Suppose there exists a prime number q such that $q \mid P(x)$ for all integers x . If b is odd then $P(0)$, and consequently q are odd; and if b is even, then since $(a, b) = 1$, a is odd; thus both $a + b$ and $a + b + 2$ are odd, and so $P(1)$ must be odd, which also implies that q is odd; hence q is odd in any case. Since it has been assumed that $q \mid P(0)$, that is $q \mid b(b + 2)$, and $q \mid P(1) + P(-1)$, it follows that $q \mid 2a^2$ and since q is odd, $q \mid a$. But this is impossible since $(a, b(b + 2)) = 1$. Hence con-

dition S is satisfied. Therefore by Conjecture H it follows that there exist infinitely many natural numbers x for which the numbers $f_1(x) = ax + b$ and $f_2(x) = ax + b + 2$ are prime. Therefore if Conjecture H is true there must be an infinite number of prime twin pairs.

That the condition $(a, b(b + 2)) = 1$ is necessary for the existence of infinitely many primes p of the form $ak + b$ for which the number $p + 2$ is also prime also follows. For if $d = (a, b(b + 2)) > 1$, then $d|a$, $d|b(b + 2)$ and since $(a, b) = 1$, it follows that $(d, b) = 1$, and so $d|(b + 2)$. But this implies that $d|ax + b + 2$ for any integer x , and so $p + 2$ would not be prime.

Conjecture H also implies that there are infinitely many quadruplets. This follows by showing that for any natural number n there are infinitely many natural numbers x for which each of the numbers

$$f_1(x) = x^{2^n} + 1, f_2(x) = x^{2^n} + 3, f_3(x) = x^{2^n} + 7, f_4(x) = x^{2^n} + 9$$

is a prime. If

$$P(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x)$$

then $P(0) = 1 \cdot 3 \cdot 7 \cdot 9$, $P(1) = 2 \cdot 4 \cdot 8 \cdot 10$ and so $(P(0), P(1)) = 1$.

Hence Condition S is satisfied and Conjecture H implies that these four polynomials are prime for infinitely many quadruplets.

Probably the most remarkable result which is implied by Conjecture H concerns the number of PAP's with any given number of terms. This results states that for any natural number n there exists infinitely many PAP's of n consecutive prime numbers. Examples of such PAP's with three terms are: 3, 5, 7; 199, 211, 223; 1499, 1511, 1523; and 4987, 4993, 4999. Examples with four terms each are 251, 257, 263, 269; 5101, 5107, 5113, 5119; and 5381, 5387, 5393, 5399. There are

none with five terms in the range less than 10 million.

The result can be formulated accurately as follows:

Statement D: If r is a natural number divisible by each prime less than or equal to n and n is a natural number greater than 1, then there exists an infinite number of systems of n consecutive prime numbers which are in an arithmetic progression with difference r .

Statement C will now be introduced. To show how Statement D follows from Conjecture H, it will be shown that Statement C follows from Conjecture H and then Statement D follows almost immediately from Statement C.

Statement C: If s is a natural number, a_1, a_2, \dots, a_s are integers such that $a_1 < a_2 < a_3 < \dots < a_s$ and if $f_i(x) = x + a_i$ for $i = 1, 2, 3, \dots, s$ satisfy Condition S, then there exists an infinite number of natural numbers x for which $f_1(x), f_2(x), \dots, f_s(x)$ are consecutive prime numbers. Proof that H implies C: The binomials $f_i(x)$ are irreducible and satisfy Condition S by hypothesis, hence by Conjecture H there exists an infinite number of natural numbers x for which each of the numbers $f_i(x)$, $i = 1, 2, 3, \dots, s$, is a prime.

Let h be one of those natural numbers such that $h \geq a_s - 2a_1 + 2$ and then let b be defined as follows:

$$b = \frac{(h + a_s)!}{(h + a_1)!(h + a_2) \dots (h + a_s)}$$

Then let $g_i(x) = bx + h + a_i$ for $i = 1, 2, 3, \dots, s$. Now

$$\begin{aligned} 2(h + a_i) &= h + h + 2a_i \\ &\geq h + h + 2a_1 \end{aligned}$$

$$\begin{aligned}
&\geq h + (a_s - 2a_1 + 2) + 2a_1 \\
&= h + a_s + 2 \\
&> h + a_s.
\end{aligned}$$

The number $h + a_i = f_i(h)$ is prime, the factors of $(h + a_s)!$ other than $h + a_i$ being less than $2(h + a_i)$ are not divisible by $h + a_i$ and hence $(b, h + a_i) = 1$.

The $g_i(x)$'s satisfy Condition S; for suppose not. That is, suppose there is a prime p such that

$$p \mid g_1(x)g_2(x)\dots g_s(x)$$

for $x = 0, 1, 2, 3, \dots, p-1$. Then

$$p \mid g_1(0) \cdot g_2(0) \dots g_s(0),$$

that is

$$p \mid (h + a_1)(h + a_2)\dots(h + a_s);$$

but since these factors are all prime there must exist a $k \leq s$ such that

$$p = h + a_k,$$

and as before

$$h + a_s < 2(h + a_k) = 2p$$

and p does not divide b . Continuing this process for $x = 1, 2, 3, \dots, p-1$

it follows that for each $i \leq s$ there exists one and only one x , where

$0 \leq x \leq p-1$, such that

$$p \mid h + a_i + bx.$$

If there were two then

$$p \mid h + a_i + bx_1 \text{ and } p \mid h + a_i + bx_2$$

and so $p \mid b(x_1 - x_2)$, but $p \nmid b$, and so $p \mid (x_1 - x_2)$, which is impossible.

Therefore

$$p \mid g_1(x)g_2(x)\dots g_s(x)$$

and since p divides exactly one $g_i(x)$ for each x there must be at least p $g_i(x)$'s, that is $p \leq s$, hence $h + a_k \leq s$. Also

$$\begin{aligned} h + a_k &> h + a_1 \\ &> a_s - a_1 + 2 \\ &> s + 1 \end{aligned}$$

which is a contradiction. Therefore the binomials $g_i(x)$ satisfy Condition S, and hence by Conjecture H there exists an infinite number of natural values of x for which the numbers $g_i(x)$, $i = 1, 2, 3, \dots, s$, are prime.

If for some x these primes were not consecutive then there would exist an integer j where $a_1 < j < a_s$, $j \neq a_i$ for any $i = 1, 2, 3, \dots, s$, such that the number

$$q = bx + h + j$$

is prime. Now since $b = (h + a_s)! / (h + a_1)!(h + a_2) \cdots (h + a_s)$ it follows that $h + j$ divides b , therefore $h + j$ divides $bx + h + j$, but this implies that $h + j$ divides q , which is prime. This is impossible, since $x > 0$.

It will now be shown how Statement C implies Statement D. Let $f_i(x) = x + ir$ for $i = 0, 1, 2, \dots, n-1$. If there exists a prime p which divides $f_0(x) \cdot f_1(x) \cdots f_{n-1}(x)$ for $x = 0, 1, 2, 3, \dots, p-1$, then by LaGrange's Theorem $p \leq n$, hence $p \mid r$. But

$$p \mid f_0(1) \cdot f_1(1) \cdots f_{n-1}(1)$$

and so $p \mid 1(1+r)(1+2r) \cdots (1+(n-1)r)$, and since $p \mid r$, it follows that $p \mid 1$, which is impossible, and so Condition S is satisfied. As a result of Statement C there exists an infinite number of natural numbers x such that the numbers $f_i(x) = x + ir$, $i = 1, 2, 3, \dots, n$, are consecutive

prime numbers. But these numbers form an arithmetic progression of n terms, and hence it follows from Conjecture H that for any natural number n there exists an infinite number of systems of n consecutive prime numbers which are in arithmetic progression.

There is a famous conjecture known as Goldbach's conjecture, which states that every even number greater than 2 is the sum of two prime numbers. Although this conjecture has not been shown to follow from Conjecture H, one very similar to it does. This is the conjecture that every even number can be represented as the difference of two primes. In fact, Conjecture H implies that every even number admits infinitely many representations as the difference of two prime numbers.

Let k denote an arbitrary integer; let $f_1(x) = x$ and $f_2(x) = x + 2k$. Then for $P(x) = f_1(x)f_2(x) = x(x + 2k)$ it follows that $P(1) = 2k + 1$ and $P(2) = 4(k + 1)$. But since $(2k + 1, 4(k + 1)) = 1$, Condition S is satisfied, and from Conjecture H it follows that there are infinitely many natural numbers x for which the number $p = x$ and $q = x + 2k$ are both prime numbers. Hence $2k = q - p$, which shows that the number $2k$ has infinitely many representations as the difference of two prime numbers.

Conjecture H also shows how to construct one prime from another in a progression-type sequence. For if $(a, b) = 1$, $a > 0$, and either a or b is even, then from Conjecture H it can be shown that there are infinitely many primes p such that $ap + b$ is also prime. Let $f_1(x) = ax + b$ and $f_2(x) = x$. With $P(x) = f_1(x) \cdot f_2(x)$ it follows that $P(1) = a + b$ and $P(-1) = a - b$. Since one of the numbers a or b is even the other must be odd, since $(a, b) = 1$, and so $(a + b, a - b) = 1$ and

Condition S is satisfied. Consequently, from Conjecture H it can be concluded that there exists infinitely many x 's for which both $ax + b$ and x are primes.

There are many other consequences which follow from Conjecture H. Whether or not these consequences will be proved independently of the conjecture, remain unsolved, be proven false, or become theorems as a result of the proof of Conjecture H is another unanswered question.

CHAPTER V

SPECIAL CASES OF DIRICHLET'S THEOREM

The primary interest in the present chapter is in the method of proof of the theorems, rather than the theorems themselves, since each is a special case of Dirichlet's general theorem. It will be seen that in some simple cases the result follows from the most elementary ideas of factorization. In other cases well-known theorems from elementary number theory help to establish the proof, while in still other cases more advanced techniques are needed. It can be noted, however, that as the a 's and the b 's of the expression $ak + b$ increase, the proofs become more complicated and more complex methods are needed to establish the result. The same is true in cases where either a or b is allowed to vary over the values such that $(a, b) = 1$.

The methods of Theorem 5.1 are similar to those used by Euclid to prove the existence of an infinite number of primes.

Theorem 5.1. There exists an infinite number of primes in the progression $4k + 3$ ($k = 0, 1, 2, 3, \dots$).

Proof: The numbers 3 and 7 are prime and are elements of the progression so the set of primes of this form is not empty.

Suppose there is only a finite number of primes in the progression, say $p_1, p_2, p_3, \dots, p_r$. Let

$$m = 4p_1p_2p_3 \dots p_r - 1 = 4(p_1p_2p_3 \dots p_r - 1) + 3.$$

Since m is a number of the progression and $m > p_i$, for each i , m must be composite and have prime factors of the form $4k + 1$ or $4k + 3$. All of the prime factors of m cannot be of the form $4k + 1$ since the product of two numbers of that form is again of that form, but m is not of that form. Therefore there must be at least one i , where $0 < i \leq r$, such that $p_i \mid m$, that is

$$p_i \mid (4p_1 p_2 p_3 \cdots p_r - 1),$$

which implies that $p_i \mid 1$, which is impossible. Since a contradiction results, the supposition must be false and hence there must be an infinite number of primes in this progression.

This type of proof will fail in many cases since the result is based upon the fact that the product of two numbers of the form $4k + 1$ is again of that form. If one attempts to prove that there are an infinite number of primes of the form $4k + 1$ by imitating this proof, trouble results. For eventually the statement that the product of two primes of the form $4k + 3$ is again of that form will be needed. This statement is false, since $(4r + 3)(4t + 3) = 16rt + 124 + 12t + 9 = 4(4rt + 3r + 3t + 2) + 1 = 4k + 1$.

The next theorem does involve primes of the form $4k + 1$, however, and again the proof is by contradiction. The contradiction is obtained from an important theorem of elementary number theory. This theorem is attributed to the famous French mathematician Pierre de Fermat.

Theorem 5.A. If p is a prime number and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary: If p is a prime number then for every integer a , $p \mid a^p - a$.

Theorem 5.2. There exists an infinite number of primes in the progression $4k + 1$ ($k = 0, 1, 2, 3, \dots$).

Proof: [18] Let n be an arbitrary natural number greater than 1 and let

$$N = (n!)^2 + 1.$$

Since $n > 1$, $n!$ is a multiple of 2, therefore N is odd and greater than 1. Let p denote the smallest prime divisor of N . Now $p > n$, for if $p \leq n$ then $p|n!$, hence $p|(n!)^2$ which implies that $p|1$, which is impossible.

Since n is odd, n is of the form $4k + 1$ or $4k + 3$. Since $p|N$, it follows that $(n!)^2 \equiv -1 \pmod{p}$. By raising each side of the congruence to the $\frac{p-1}{2}$ -th power it follows that

$$(n!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

But $p \nmid (n!)$, so by Fermat's theorem

$$(n!)^{p-1} \equiv 1 \pmod{p}$$

and by the transitive property for congruences

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

If p is of the form $4k + 3$, then $\frac{p-1}{2} = 2k + 1$ would be odd and then

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \equiv 1 \pmod{p}$$

which implies that $p|2$, that is, $p = 2$, but this is impossible since N is odd and 2 cannot divide N . Therefore p must be of the form $4k + 1$. It follows that for every natural number $n > 1$ there exists a prime p greater than n of the form $4k + 1$. In fact, every prime divisor of N is such a prime. Since n is arbitrary, the theorem follows.

The proofs of the first two theorems are quite simple because it is only necessary to consider primes not of the form under consideration. In each case there was only one other form to consider. In the next theorems primes of the form $8k + 7$ and $8k + 3$ are considered. If a prime $p > 2$ is not of the form $8k + 7$, then it could be of the form $8k + 1$, $8k + 3$, or $8k + 5$. Other procedures than those used in Theorems 5.1 and 5.2 must be used. Before attempting the proofs the necessary theorems and definitions from elementary number will again be given.

Definition 5.1: Quadratic Residue. If p is an odd prime with $(n, p) = 1$ and the congruence $x^2 \equiv n \pmod{p}$ is solvable, then n is called a quadratic residue modulo p . Otherwise n is called a quadratic non-residue modulo p .

Definition 5.2: Legendre Symbol. If p is an odd prime and $(n, p) = 1$, then the symbol $\left(\frac{n}{p}\right)$ is defined by the following equations.

$$\left(\frac{n}{p}\right) = 1 \text{ if } n \text{ is a quadratic residue modulo } p.$$

$$\left(\frac{n}{p}\right) = -1 \text{ if } n \text{ is a quadratic non-residue modulo } p.$$

Theorem 5.B. If m and n are integers and neither is divisible by p , then

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right)$$

Theorem 5.C. Euler's Criterion. If p is an odd prime $(p, n) = 1$, then

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p} \text{ and } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Theorem 5.D. If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

The plan of the proof is similar to that of Theorem 5.2. For every natural number n it will be shown that there is a prime larger than n in the progression. Since there are an infinite number of n 's which can be considered, there must be an infinite number of primes in the progression.

Theorem 5.3. There exists an infinite number of primes in the progression $8k + 7$ ($k = 0, 1, 2, 3, \dots$).

Proof: The progression can be represented $8k - 1$ ($k = 1, 2, \dots$). Let n be any natural number greater than 1 and consider the number

$$N = 2(n!)^2 - 1.$$

Since $n > 1$, it follows that $N > 1$ and therefore must have at least one odd prime divisor p which is not of the form $8k + 1$. The reason is that the product of two numbers of the form $8k + 1$ is again of that form but N is of the form $8k - 1$. Since $p \mid N$ it follows that

$$2(n!)^2 \equiv 1^2 \pmod{p},$$

and so $2(n!)^2$ is a quadratic residue modulo p . By Theorem 5.8 the following equalities are obtained.

$$\left(\frac{2(n!)^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{n!}{p}\right)^2 = \left(\frac{2}{p}\right) = 1$$

Theorem 5.D and the preceding equalities imply that $\frac{p^2-1}{8}$ is even, therefore p must be of the form $8k \pm 1$. But it has been shown that p is not of the form $8k + 1$, so it must be of the form $8k - 1$. Also since

$p \mid (2(n!)^2 - 1)$ it follows that $p > n$. If not, then as before, p would divide 1. So for every natural number $n > 1$ there exists a prime p greater than n of the form $8k - 1$. Since n is arbitrary, the proof is completed.

The plan of the proof of the next theorem is similar to the preceding one but the theorems from elementary number theory are used in a slightly different manner.

Theorem 5.4. There exists an infinite number of primes in the progression $8k + 3$ ($k = 0, 1, 2, 3, \dots$).

Proof: Let n be a natural number greater than 1 and let $a = p_1 p_2 p_3 \cdots p_n$ be the product of the first n odd prime numbers. Since a is odd, its square, a^2 , is of the form $8t + 1$. Let

$$N = a^2 + 2.$$

N is therefore of the form $8t + 3$. If every prime divisor of N were of the form $8t + 1$, then N would be of that form. Since it is not, N must have at least one prime divisor p of the form $8k + 3$ or $8k + 5$. Suppose p were of the form $8k + 5$. Since $p \mid N$ and $N = a^2 + 2$ it follows that

$$a^2 \equiv -2 \pmod{p}$$

and so $\left(\frac{-2}{p}\right) = 1$. But Theorems 5.B, 5.C and 5.D imply that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}$$

Since $p = 8k + 5$, $p - 1 = 8k + 4$ and $\frac{p-1}{2} = 4k + 2$ is even and

$p^2 = 64k^2 + 80k + 25$ which implies that $\frac{p^2-1}{8} = 8k^2 + 10k + 3$ is odd.

Therefore the following equalities are obtained.

$$1 = \left(\frac{-2}{p}\right) = (-1)^{\text{even}} (-1)^{\text{odd}} = -1 \cdot 1 = -1$$

This is obviously a contradiction, therefore p must not be of the form $8k + 5$, that is, it must be of the form $8k + 3$. Now $p \mid a^2 + 2$ and $a = p_1 p_2 p_3 \cdots p_n$ where each p_i is odd. Hence $p > p_i$ for each i , $1 \leq i \leq n$. Since n may be chosen arbitrarily large the theorem is proved.

A proof for the sequence with elements of the form $8k + 5$ follows similarly by choosing $N = a^2 + 4$.

With the exception of the proof of the case $8k + 1$, and details of the case $8k + 5$, it has been shown that there is an infinite number of primes of the form $8k + b$, where $(8, b) = 1$. The case for the progression with terms of the form $8k + 1$ is a special case of Theorem 5.8. After the proof of this theorem we will have established Dirichlet's Theorem for the case $8k + b$, where $(8, b) = 1$.

All of the proofs thus far have involved only the very fundamentals of elementary number theory, and yet one of the more well-known theorems of the subject has not been used. This theorem is referred to as the quadratic reciprocity law of Gauss. It is probably called a law since a proof of it was not given until ten years after it had been discovered. Euler and Legendre are given credit for its discovery in 1785. Gauss rediscovered it in 1885 when he was only 18 years of age. The first proof was given by Gauss, who writes of his initial effort:

For a whole year this theorem tormented me and absorbed my greatest efforts until, at last, I obtained a proof ... [13: 82]

Eventually Gauss devised seven different proofs and since that time

several more have been added.

The next proof will use the quadratic reciprocity law but the basic plan of the proof is similar to the preceding ones in that a prime of the desired form is shown to exist larger than any preassigned natural number n .

Theorem 5.E. Quadratic Reciprocity Law. If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Theorem 5.5. There exists an infinite number of primes in the progression $5k + 1$ ($k = 1, 2, 3, \dots$).

Proof: Let n be an arbitrary natural number greater than 1. Let

$$N = 5(n!)^2 + 1.$$

N is odd, N is greater than 1, and N is not of the form $5t + 1$. N must therefore have at least one prime divisor p , which is odd, is not 5, and is not of the form $5t + 1$. If $p \leq n$ then $p \mid (n!)^2$ and therefore $p \mid 1$, which is impossible, hence $p > n$. Since $p \mid N$ it follows that

$$5(n!)^2 \equiv -1 \pmod{p}$$

and so $\left(\frac{5}{p}\right) = 1$. The quadratic reciprocity law gives

$$\left(\frac{5}{p}\right) \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} = 1$$

and therefore $\left(\frac{p}{5}\right) = 1$. Since $p \neq 5$, p must be of the form $5k + 1$ or $5k + 2$. If $p = 5k + 2$, then by Theorems 5.B, 5.C, and 5.D, it follows that

$$\left(\frac{p}{5}\right) = \left(\frac{+2}{-5}\right) = \left(\frac{+1}{5}\right) \left(\frac{2}{5}\right) = 1 \cdot -1 = -1$$

which is a contradiction, therefore p must be of the form $5k + 1$. It has been shown that it is not of the form $5k + 1$ and so the only remaining possibility is for p to be of the form $5k - 1$. Thus for any natural number n there is a prime p greater than n and of the form $5k - 1$. Since n can be chosen arbitrarily large, there must be an infinite number of primes of this form.

The next theorem is Dirichlet's Theorem for all progressions with common difference between successive terms equal to 24. It appears that the theorem considers an infinite number of progressions, however, every progression of the form $24k + b$ ($k = 0, 1, 2, 3, \dots$), where $(24, b) = 1$, is a sub-sequence of the progression $24k + b'$ where $b' < 24$ and $b \equiv b' \pmod{24}$. It is therefore sufficient to prove the theorem for specific cases of b , that is, for those b 's less than 24 such that $(24, b) = 1$.

The plan of the proof, which is due to Bateman and Low [2], is this. For each value of b a certain polynomial in P will be considered, where P is the product of any finite set S of primes each greater than 24. From the divisibility properties of the polynomial it will be shown that S cannot possibly contain all primes greater than 24 in the progression $24k + b$, and so the number of primes in the progression will have to be infinite in number.

The proof is based upon the following four lemmas.

Lemma 1. Let p be a prime number greater than 3. Then

$$\left(\frac{-1}{p}\right) = 1 \text{ if and only if } p \equiv 1 \pmod{4},$$

$$\left(\frac{2}{p}\right) = 1 \text{ if and only if } p \equiv 1, 7 \pmod{8},$$

$$\left(\frac{-2}{p}\right) = 1 \text{ if and only if } p \equiv 1, 3 \pmod{8},$$

$$\left(\frac{3}{p}\right) = 1 \text{ if and only if } p \equiv 1, 11 \pmod{12},$$

$$\left(\frac{-3}{p}\right) = 1 \text{ if and only if } p \equiv 1 \pmod{6},$$

$$\left(\frac{6}{p}\right) = 1 \text{ if and only if } p \equiv 1, 5, 19, 23 \pmod{24},$$

$$\left(\frac{-6}{p}\right) = 1 \text{ if and only if } p \equiv 1, 5, 7, 11 \pmod{24}.$$

Proof: The proofs follow from Theorems 5.A-5.E. The first statement follows directly from Theorem 5.C. The second follows from Theorem 5.D and the fact that $\frac{p^2-1}{8}$ is even when $p \equiv 1, 7 \pmod{8}$, and is odd when $p \equiv 3, 5 \pmod{8}$. For the third statement the following fact is used.

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = 1 \text{ iff } \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1 \text{ or } \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

In the first case $p \equiv 1 \pmod{4}$ and $p \equiv \pm 1 \pmod{8}$. If $p \equiv -1 \pmod{8}$, then $p \equiv -1 \pmod{4}$ and thus $p \equiv 1 \equiv -1 \pmod{4}$ which implies that $4|2$, which is not true, and so $p \equiv 1 \pmod{8}$. In the second case $p \equiv 3 \pmod{4}$ and $p \equiv \pm 3 \pmod{8}$. Now if $p \equiv -3 \pmod{8}$, then $p \equiv -3 \pmod{4}$ and thus $p \equiv 3 \equiv -3 \pmod{4}$ which implies that $4|6$, which is false, and so $p \equiv 3 \pmod{8}$. By Theorem 5.E.

$$\left(\frac{3}{p}\right) \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$$

and so

$$\begin{aligned}\left(\frac{3}{p}\right) &= \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) \text{ if } p \equiv 1 \pmod{4} \\ &= -\left(\frac{p}{3}\right) \text{ if } p \equiv 3 \pmod{4}.\end{aligned}$$

Since $\left(\frac{p}{3}\right) = \left(\frac{r}{3}\right)$ where r is the least residue of p modulo 3, it follows that

$$\begin{aligned}\left(\frac{p}{3}\right) &= \left(\frac{1}{3}\right) = 1 \text{ if } p \equiv 1 \pmod{3} \\ &= -1 \text{ if } p \equiv 2 \pmod{3}.\end{aligned}$$

Therefore the following congruences hold.

$$\begin{aligned}\left(\frac{3}{p}\right) &= 1 \text{ if } p \equiv 1 \pmod{4} \text{ and } p \equiv 1 \pmod{3}, \\ &= 1 \text{ if } p \equiv 3 \pmod{4} \text{ and } p \equiv 2 \pmod{3}, \\ &= -1 \text{ if } p \equiv 1 \pmod{4} \text{ and } p \equiv 2 \pmod{3}, \\ &= -1 \text{ if } p \equiv 3 \pmod{4} \text{ and } p \equiv 1 \pmod{3}.\end{aligned}$$

By the Chinese Remainder theorem:

$$\begin{aligned}p &\equiv 1 \pmod{4} \text{ and } p \equiv 1 \pmod{3} \text{ imply } p \equiv 1 \pmod{12}, \\ p &\equiv 3 \pmod{4} \text{ and } p \equiv 2 \pmod{3} \text{ imply } p \equiv 11 \equiv -1 \pmod{12}, \\ p &\equiv 1 \pmod{4} \text{ and } p \equiv 2 \pmod{3} \text{ imply } p \equiv 5 \pmod{12}, \\ p &\equiv 3 \pmod{4} \text{ and } p \equiv 1 \pmod{3} \text{ imply } p \equiv 7 \equiv -5 \pmod{12}.\end{aligned}$$

The above conclusions can be summarized by

$$\begin{aligned}\left(\frac{3}{p}\right) &= 1 \text{ if } p \equiv \pm 1 \equiv 1, 11 \pmod{12} \\ &= -1 \text{ if } p \equiv \pm 5 \equiv 5, 7 \pmod{12}.\end{aligned}$$

The proof of the fifth statement is similar to the proof of the third statement and statements six and seven follow in the same manner as four and five.

Lemma 2. If n is any integer, then any prime factor of $n^8 - n^4 + 1$ is congruent to 1 modulo 24.

Proof: It is sufficient to prove the statement for $n \geq 2$ since the exponents of the polynomial are even and if $n = 0$ or $n = 1$ the polynomial takes on the value 1 and there are no prime factors. Suppose $n > 1$ and $p \mid n^8 - n^4 + 1$, that is

$$n^8 - n^4 + 1 \equiv 0 \pmod{p}.$$

Now $p \neq 2$, since the polynomial is odd. Also $p \neq 3$, for if it did, then by Fermat's Theorem (Theorem 5.A),

$$n^2 \equiv 1 \pmod{3}$$

and hence

$$n^8 \equiv 1 \pmod{3} \text{ and } n^4 \equiv 1 \pmod{3}$$

which imply that

$$n^8 - n^4 \equiv 0 \pmod{3}$$

which is impossible since $n^8 - n^4 \equiv -1 \pmod{3}$ and $0 \not\equiv -1 \pmod{3}$.

Therefore $p > 3$. Since

$$n^8 - n^4 = n^2(n^6 - n^2) = n^2(n^3 - n)(n^3 + n) \equiv -1 \pmod{p}$$

it follows that

$$(p, n^2) = (p, n^3 - n) = (p, n^3 + n) = 1.$$

The congruence $a_0 x \equiv 1 \pmod{p}$ has a solution if and only if $(a_0, p) = 1$, and so there must exist integers a , b , and c , such that

$$(1) \quad an^2 \equiv 1 \pmod{p},$$

$$(2) \quad b(n^3 + n) \equiv 1 \pmod{p},$$

$$(3) \quad c(n^3 - n) \equiv 1 \pmod{p},$$

Since $n^8 - n^4 + 1 = (n^4 - 1)^2 + (n^2)^2$ the congruence

$$a^2(n^8 - n^4 + 1) \equiv 0 \pmod{p}$$

implies that

$$a^2(n^4 - 1)^2 + a^2n^4 \equiv 0 \pmod{p}$$

which gives

$$a^2n^8 - 2a^2n^4 + a^2 + a^2n^4 \equiv 0 \pmod{p}$$

and since $a^2n^4 \equiv 1 \pmod{p}$, it follows that

$$(4) \quad (an^4 - a)^2 + 1 \equiv 0 \pmod{p}.$$

By algebraic manipulation the following equalities are obtained.

$$(5) \quad n^8 - n^4 + 1 = (n^4 + n^2 + 1)^2 - 2(n^3 + n)^2$$

$$(6) \quad = (n^4 - n^2 + 1)^2 + 2(n^3 - n)^2$$

$$(7) \quad = (n^4 + 1)^2 - 3(n^2)^2$$

$$(8) \quad = (n^4 - \frac{1}{2})^2 + 3(\frac{1}{2})^2$$

$$(9) \quad = (n^4 + 3n^2 + 1)^2 - 6(n^3 + n)^2$$

$$(10) \quad = (n^4 - 3n^2 + 1)^2 + 6(n^3 - n)^2.$$

By using methods similar to those used to derive (4) it can be verified that

$$(2) \text{ and } (5) \text{ imply } (bn^4 + bn^2 + b)^2 - 2 \equiv 0 \pmod{p},$$

$$(3) \text{ and } (6) \text{ imply } (cn^4 - cn^2 + c)^2 + 2 \equiv 0 \pmod{p},$$

$$(1) \text{ and } (7) \text{ imply } (an^4 + a)^2 - 3 \equiv 0 \pmod{p},$$

Multiplying (8) by 2^2 , $(2n^4 - 1)^2 + 3 \equiv 0 \pmod{p}$ is obtained,

$$(2) \text{ and } (9) \text{ imply } (bn^4 + 3bn^2 + b)^2 - 6 \equiv 0 \pmod{p},$$

$$(3) \text{ and } (9) \text{ imply } (cn^4 - 3cn^2 + c)^2 + 6 \equiv 0 \pmod{p}.$$

The preceding six congruences and (4) imply the following equalities.

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-6}{p}\right) = 1$$

and so by Lemma 1, $p \equiv 1 \pmod{24}$.

In the following lemma the following polynomials are used.

$$f_5(x) = x^4 + 9 = (x^2)^2 + 3^2 = (x^2+3)^2 - 6x^2 = (x^2-3)^2 + 6x^2$$

$$f_7(x) = x^4 + 2x^2 + 4 = (x^2+2)^2 - 2x^2 = (x^2+1)^2 + 3 = (x^2-2)^2 + 6x^2$$

$$f_{11}(x) = x^4 + 4x^2 + 1 = (x^2+1)^2 + 2x^2 = (x^2+2)^2 - 3 = (x^2-1)^2 + 6x^2$$

$$f_{13}(x) = x^4 - x^2 + 1 = (x^2-1)^2 + x^2 = (x^2-\frac{1}{2})^2 + 3(\frac{1}{2})^2 = (x^2+1)^2 - 3x^2$$

$$f_{17}(x) = x^4 + 1 = (x^2)^2 + 1 = (x^2+1)^2 - 2x^2 = (x^2-1)^2 + 2x^2$$

$$f_{19}(x) = x^4 - 2x^2 + 1 = (x^2-1)^2 + 2x^2 = (x^2-1)^2 + 3 = (x^2+2)^2 - 6x^2$$

$$f_{23}(x) = x^4 - 4x^2 + 1 = (x^2-1)^2 - 2x^2 = (x^2-2)^2 - 3 = (x^2+1)^2 - 6x^2$$

Lemma 3. Suppose b is one of the numbers 5, 7, 11, 13, 17, 19, 23. Suppose n is an integer and p is a prime number greater than three. If $f_b(n) \equiv 0 \pmod{p}$, then $p \equiv 1 \pmod{24}$ or $p \equiv b \pmod{24}$.

Proof: The proof follows from Lemma 1 and the corresponding identities for $f_b(x)$. Only the cases for $b = 19$ and $b = 13$ will be given.

If $b = 19$ and $f_{19}(n) \equiv 0 \pmod{p}$, where $p > 3$, then

$$(n^2 - 2)^2 + 2n^2 \equiv (n^2 - 1)^2 + 3 \equiv (n^2 + 2)^2 - 6n^2 \equiv 0 \pmod{p}.$$

Hence the congruences

$$x^2 \equiv -2n^2 \pmod{p}$$

$$x^2 \equiv -3 \pmod{p}$$

$$x^2 \equiv 6n^2 \pmod{p}$$

each have a solution in the integers. Therefore

$$\left(\frac{-2n^2}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{n}{p}\right)^2 = \left(\frac{-2}{p}\right) = 1,$$

$$\left(\frac{-3}{p}\right) = 1, \text{ and}$$

$$\left(\frac{6n^2}{p}\right) = \left(\frac{6}{p}\right)\left(\frac{n}{p}\right)^2 = \left(\frac{6}{p}\right) = 1$$

Therefore, by Lemma 1, $p \equiv 1, 5, 19, 23 \pmod{24}$, since $\left(\frac{6}{p}\right) = 1$. But if $p \equiv 5 \pmod{24}$, then $p \equiv 5 \pmod{8}$ and this is ruled out since $\left(\frac{-2}{p}\right) = 1$. (See Lemma 1). If $p \equiv 23 \pmod{24}$, then $p \equiv 5 \pmod{6}$ and this is impossible since $\left(\frac{-3}{p}\right) = 1$. Therefore $p \equiv 1 \pmod{24}$ or $p \equiv 19 \pmod{24}$.

If $b = 13$ and $f_{13}(n) \equiv 0 \pmod{p}$, with $p > 3$, then the term involving $\frac{1}{2}$ of $f_{13}(n)$ must be multiplied by 2^2 , and then it follows that $(n^2 - 1)^2 + n^2 \equiv 2^2(n^2 - \frac{1}{2})^2 + 2^2(3)(\frac{1}{2})^2 \equiv (n^2 + 1)^2 - 3n^2 \equiv 0 \pmod{p}$,

and as before:

$$\left(\frac{-n^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right)^2 = \left(\frac{-1}{p}\right) = 1, \left(\frac{-3}{p}\right) = 1 \text{ and}$$

$$\left(\frac{3n^2}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{n}{p}\right)^2 = \left(\frac{3}{p}\right) = 1, \text{ and by checking the possi-}$$

bilities of Lemma 1, it follows that $p \equiv 1 \pmod{24}$ or $p \equiv 13 \pmod{24}$.

The other five cases follow similarly.

In the next lemma and the main theorem polynomials are again used. The importance of each polynomial is in the fact that the constant term of each one is one of the b 's under consideration and the other coefficients are integers which are divisible by 24. The

polynomials are:

$$g_5(x) = \frac{1}{2}f_5(12x+1) = 24(432x^4 + 144x^3 + 18x^2 + x) + 5$$

$$g_7(x) = f_7(6x+1) = 24(54x^4 + 36x^3 + 12x^2 + 2x) + 7$$

$$g_{11}(x) = \frac{1}{3}f_{11}(6x+2) = 24(18x^4 + 24x^3 + 14x^2 + 4x) + 11$$

$$g_{13}(x) = f_{13}(12x+2) = 24(864x^4 + 576x^3 + 138x^2 + 14x) + 13$$

$$g_{17}(x) = f_{17}(6x+2) = 24(54x^4 + 72x^3 + 36x^2 + 8x) + 17$$

$$g_{19}(x) = \frac{1}{12}f_{19}(12x+4) = 24(72x^4 + 96x^3 + 47x^2 + 10x) + 19$$

$$g_{23}(x) = \frac{1}{2}f_{23}(12x+3) = 24(432x^4 + 432x^3 + 150x^2 + 21x) + 23$$

Lemma 4. If b is one of the numbers 5, 7, 11, 13, 17, 19, 23, and n is any integer, then $g_b(n)$ has at least one prime factor which is congruent to b modulo 24.

Proof: From the way the $g_b(x)$'s were defined it follows that

$g_b(n) \equiv b \pmod{24}$, since $g_b(n) = P + b$ where P is some polynomial in

n . Also, $g_b(n)$ is not divisible by 2 or 3, for if it were then b would

be divisible by 2 or 3, but b is a prime greater than 3. Since $g_b(x)$

is defined in terms of $f_b(y)$ where y is also an integer defined in terms

of x , Lemma 3 applies, and so all prime factors of $g_b(n)$ are congruent

to 1 or to b modulo 24. If all prime factors of $g_b(n)$ were congruent to

1 modulo 24, then all powers and products of these primes would also

be congruent to 1 modulo 24 and thus $g_b(n)$ would be congruent to

b modulo 24. If this is the case then $b \equiv 1 \pmod{24}$, but $1 < b < 24$

and so the congruence is impossible. Thus there must be at least one

prime divisor p of $g_b(n)$ which is congruent to b modulo 24.

The main theorem can now be proved.

Theorem 5.6. There exists an infinite number of primes in the progression $24k + b$ ($k = 0, 1, 2, 3, \dots$), where $(24, b) = 1$.

Proof: Since b is fixed it can be assumed that b is one of the numbers 1, 5, 7, 11, 13, 17, 19, 23. If $b > 24$, and $(24, b) = 1$, then the progression is the same as one with the first term listed, less a finite number of terms.

Let S be any non-empty finite set of primes each element of which is greater than 24. That is $S = \{p_1, p_2, \dots, p_r\}$ where $p_i > 24$, for each i . Let $p = p_1 \cdot p_2 \cdots p_r$. Therefore $p > 1$, and by Lemma 2, each prime factor of $p^8 - p^4 + 1$ is congruent to 1 modulo 24 but different from any of the primes in S . If some p_i in S were a factor of the polynomial then it would have to be a factor of 1, which is impossible. So each factor of $p^8 - p^4 + 1$ is greater than each prime in S and each is congruent to 1 modulo 24. That is, each is of the form $24k + 1$. Since S can be chosen to include any number of elements, there must be an infinite number of primes of the form $24k + 1$.

The proof for each $b \neq 1$ follows by using the g_b polynomials. If b is one of the numbers 5, 7, 11, 13, 19, or 23, choose a positive integer c_b such that

$$g_b(c_b) \not\equiv 0 \pmod{b}.$$

Such a c_b exists, for each b , because b is prime and since the leading coefficient of $g_b(x)$ is not divisible by b the polynomial cannot have more zeros than its degree. In fact c_b can be described numerically as follows:

$$c_5 = 2, \quad c_7 = 1, \quad c_{11} = 1, \quad c_{13} = 1, \quad c_{17} = 2, \quad \text{and} \quad c_{23} = 2.$$

The positive integer, $g_b(c_b P^{b-1})$, has at least one prime factor

which is congruent to b modulo 24, by Lemma 4. Since b is a prime less than 24 it follows that $(b, P) = 1$. The constant term of $g_b(x)$ is b and so each term of $g_b(c_b P^{b-1})$ except the constant term is divisible by each prime in S . Now b is not divisible by any prime in S and so $g_b(c_b P^{b-1})$ is not divisible by any prime in S . By Fermat's Theorem

$$g_b(c_b P^{b-1}) \equiv g_b(c_b) \not\equiv 0 \pmod{b}$$

and so $g_b(c_b P^{b-1})$ is not divisible by b . The following has been shown:

- (1) $g_b(c_b P^{b-1})$ has a prime factor which is congruent to b modulo 24.
- (2) This prime factor is not b .
- (3) This prime factor is different from any prime in S .

If there is only a finite number of primes in the progression under consideration, then let S be that finite set. Then there exists a prime factor of $g_b(c_b P^{b-1})$ which is in the progression, is not b , and is not in S . Therefore S did not include all such primes, and so there must be an infinite number of primes in the progression.

Before proving a more general theorem concerning the primes in an arithmetic progression the equivalence of the following two statements is needed.¹

Statement T_0 . If a and b are natural numbers such that $(a, b) = 1$, then there exists an infinite number of primes in the progression

¹The proof of the equivalence of T_0 and T_1 was given by Sierpinski in 1950. Six years later the problem of the equivalence of T_0 and T_1 was formulated in The American Mathematical Monthly as E 1218 (1956) p. 342; and solved by D. Zeitlin (1957) p. 46.

$ak + b$ ($k = 1, 2, 3, \dots$).

Statement T_1 . If a and b are natural numbers such that $(a, b) = 1$, then there exists at least one prime number p in the progression $ak + b$, where k is a natural number.

T_0 is Dirichlet's Theorem, while T_1 merely states the existence of one prime in the progression. If T_0 and T_1 are equivalent, then if one wishes to prove the existence of an infinite number of primes in the arithmetic progression $ak + b$, where $(a, b) = 1$, it is sufficient to prove the existence of one prime in each of the progressions of this form.

Theorem 5.F. T_0 and T_1 are equivalent.

Proof: Trivially T_0 implies T_1 . It is sufficient to prove the converse, that is T_1 implies T_0 .

Let a and b be any natural numbers such that $(a, b) = 1$. By T_1 there exists a natural number k_1 such that $ak_1 + b$ is prime. Then $(a, ak_1 + b) = 1$ and by T_1 again there exists a k_2 such that $ak_2 + (ak_1 + b) = a(k_1 + k_2) + b$ is prime. Continuing this process, it follows that $ak + b$ is prime for infinitely many values.

The following theorem concerns primes in the progression with first term 1 and common difference which is 2 times some power of a prime. The method of proof uses more ideas from elementary number theory to prove the existence of one prime in the progression. One definition and one more theorem are needed for the proof.

Definition 5.3. If t is the least positive integer such that $n^t \equiv 1 \pmod{r}$, then n is said to belong to the exponent t modulo r .

Theorem 5.6. If $(a, m) = 1$, then any solution of $a^x \equiv 1 \pmod{m}$ is divisible by the exponent t to which a belongs with respect to the modulus, and in particular $t \mid \phi(m)$, where ϕ is the well-known Euler ϕ -function.

The next theorem considers the progressions of the form $2p^s k + 1$, where s is any natural number. The proof follows by considering a polynomial of the form $a^{p-1} + a^{p-2} + \dots + 1$ where $a = 2^{p^{s-1}}$, and showing that any prime divisor of the polynomial has the form $2p^s k + 1$.

Theorem 5.7. If p is a prime and s is a natural number, then there is an infinite number of primes in the progression $2p^s k + 1$ ($k = 1, 2, 3, \dots$).

Proof: Let p be a prime and let s be any natural number. Let

$$a = 2^{p^{s-1}}$$

and let q be an arbitrary prime divisor of the number

$$a^{p-1} + a^{p-2} + a^{p-3} + \dots + a + 1.$$

The fact that $a \not\equiv 1 \pmod{q}$ is needed. Suppose $a \equiv 1 \pmod{q}$. Then

$$a^2 \equiv 1 \pmod{q},$$

$$a^3 \equiv 1 \pmod{q},$$

$$\vdots$$

$$a^{p-1} \equiv 1 \pmod{q},$$

and summing the congruences

$$a^{p-1} + a^{p-2} + a^{p-3} + \dots + a + 1 \equiv 1 + 1 + \dots + 1 \equiv p \pmod{q}$$

is obtained. Since q is a factor of $a^{p-1} + a^{p-2} + \dots + a + 1$ it follows that $q \mid p$, and in view of the fact that q and p are both primes, $p = q$. Also if $a \equiv 1 \pmod{p}$, it follows that $a^p \equiv a \equiv 1 \pmod{p}$, where $a = 2^{p^{s-1}}$. Therefore

$$(2^{p^{s-1}})^p = 2^{p^s} \equiv 1 \pmod{p}.$$

By the corollary to Theorem 5.A, it follows that

$$2^p \equiv 2 \pmod{p},$$

and by induction

$$2^{p^s} \equiv 2 \pmod{p},$$

hence

$$1 \equiv 2^{p^s} \equiv 2 \pmod{p}$$

which is impossible, so $a \not\equiv 1 \pmod{q}$.

Let t denote the exponent to which 2 belongs with respect to the modulus q . By hypothesis

$$a^{p-1} + a^{p-2} + \dots + a + 1 \equiv 0 \pmod{q}$$

and multiplying by a ,

$$a^p + a^{p-1} + \dots + a^2 + a \equiv 0 \pmod{q}$$

is obtained. From this it follows that

$$a^p \equiv 1 \pmod{q},$$

that is

$$2^{p^s} \equiv 1 \pmod{q}.$$

By Theorem 5.G, $t \mid p^s$ and since $2^{p^{s-1}} \not\equiv 1 \pmod{p}$, $t \nmid p^{s-1}$, and hence $t = p^s$. Since $t \mid \phi(q)$ and $\phi(q) = q - 1$, it follows that $p^s \mid (q-1)$. Since $2^{p^s} \equiv 1 \pmod{q}$, q must be odd and $q-1$ is therefore even. If p is a prime number greater than 2, then $(2, p) = 1$, and hence

$2p^s \mid (q-1)$, which shows that

$$q = 2p^s k + 1$$

for some natural number k . If $p = 2$, then $2^s \mid (q-1)$ and

$$q = 2^s k + 1$$

for some natural number k . So if p is prime then there is a prime number of the form $2p^s k + 1$. Since T_0 is equivalent to T_1 , the theorem is proved.

The next and final proof of a special case of Dirichlet's Theorem that will be given is even more general than the preceding one. The progressions under discussion are those with first term 1 and common difference any natural number.

The proof follows by considering the expression $n^n - 1$. This expression is shown to have a prime divisor that belongs to the exponent n with respect to the modulus p . Then Fermat's Theorem is used to show that this n is a factor of $p-1$, and hence p is of the form $nk + 1$. The difficult part of the proof is in showing that $n^n - 1$ has a prime divisor belonging to the exponent n .

The reader is reminded of the definition of the Möbius function and one more basic theorem from elementary number theory.

Definition 5.4. Möbius Function: The Möbius function μ is defined on the set of natural numbers as follows:

$$\mu(1) = 1$$

$$\mu(n) = (-1)^r, \text{ if } n = p_1 p_2 \cdots p_r \text{ where the } p_i \text{'s are distinct odd primes.}$$

$$\mu(n) = 0 \text{ if } p^2 \mid n \text{ for any prime } p.$$

Theorem 5.H. $\sum_{d|n} \mu(d) = 1$ if $n = 1$
 $= 0$ if $n > 1$.

Theorem 5.8. For every natural number n , there exists an infinite number of primes in the progression $nk + 1$ ($k = 1, 2, \dots$).

Proof: [19] By the equivalence of T_0 and T_1 it is sufficient to show that for any natural number n there exists at least one prime number of the form $nk + 1$, where k is any natural number.

If $n = 1$, then the progression consists of all natural numbers greater than 1 and therefore the theorem holds. If $n = 2$, then the progression consists of all odd numbers greater than 2 and this set also has an infinite number of primes. Therefore assume that $n > 2$.

Let $n = q_1^{a_1} q_2^{a_2} \dots q_r^{a_r}$ be the canonical representation of n where $q_1 < q_2 < \dots < q_r$. Suppose that for every prime divisor of the number $n^n - 1$, the number n belongs to an exponent less than n with respect to the modulus p . It will be shown that this is impossible.

Let

$$P_n = \prod_{d|n} (n^d - 1)^{\mu(\frac{n}{d})}$$

where μ is the Möbius function. Then for every divisor d , represent each of the factors $(n^d - 1)$ as the product of its prime factors. The exponent of any factor is an integer, either positive, negative, or zero. Let p_0 be one of those prime factors. Then there exists a natural number d such that $d|n$ and $p_0 | (n^d - 1)$, that is $n^d \equiv 1 \pmod{p_0}$. Therefore

$$(n^d)^s = n^{ds} = n^n \equiv 1^s \equiv 1 \pmod{p_0},$$

and $(n, p_0) = 1$. Let t denote the exponent to which n belongs with

respect to the modulus p_0 . Then by hypothesis it follows that $t < n$. Now among the numbers $(n^d - 1)$, where $d|n$, $p_0|(n^d - 1)$ if and only if $t|d$. The only if part follows from Theorem 5.G.

If $t|d$, let $tk = d$. Then

$$n^d = n^{tk} = (n^t)^k \equiv 1^k \equiv 1 \pmod{p_0},$$

and so $p_0|(n^d - 1)$. Hence the numbers $n^d - 1$ are divisible by p_0 for precisely those d 's for which $t|d$, that is, for those for which $d = tk$, where k is a natural number such that $tk|n$. Since $t|n$, $k|\frac{n}{t}$, where $\frac{n}{t}$ is a natural number greater than 1 because $t < n$.

Let s be the greatest exponent for which $p_0^s|(n^t - 1)$, that is $p_0^{s+1} \nmid (n^t - 1)$. It will be shown that s is the largest exponent such that $p_0^s|(n^{kt} - 1)$, where $k|\frac{n}{t}$. For suppose $p_0^{s+1} \mid (n^{kt} - 1)$. Then consider the following identity.

$$\frac{n^{kt} - 1}{n^t - 1} = \left[(n^t)^{k-1} - 1 \right] + \left[(n^t)^{k-2} - 1 \right] + \dots + \left[n^t - 1 \right] + k.$$

Since p_0 divides the left side of the equality it must also divide the right side, but p_0 also divides each term of the right side which is in brackets, and hence $p_0|k$. This is impossible since $k|\frac{n}{t}$ and $(n, p_0) = 1$. Therefore s is the largest exponent such that $p_0^s|(n^{kt} - 1)$.

From the preceding, it follows that in the factorization of P_n the exponent of the prime p_0 is

$$\sum_{k|\frac{n}{t}} s \cdot \mu\left(\frac{n}{tk}\right).$$

But since $\frac{n}{t}$ is a natural number greater than 1, Theorem 5.H implies the following:

$$\sum_{k|\frac{n}{t}} \mu\left(\frac{n}{tk}\right) = \sum_{k|\frac{n}{t}} \mu(k) = 0.$$

Since this is valid for any prime factor of P_n , it follows that $P_n = 1$.

Now

$$P_n = \prod_{d|n} (n^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|q_1 q_2 \dots q_r} (n^{\frac{n}{d}} - 1)^{\mu(d)}$$

because $\mu(d) = 0$ when d is divisible by the square of a natural number greater than 1. Let $b = n^{q_1^{a_1-1} : q_2^{a_2-1} : \dots : q_r^{a_r-1}}$. Therefore

$b \geq n \geq 2$ and

$$\begin{aligned} b^{q_1 q_2 \dots q_r} &= (n^{q_1^{a_1-1} q_2^{a_2-1} \dots q_r^{a_r-1}})^{q_1 q_2 \dots q_r} \\ &= n^{q_1^{a_1} q_2^{a_2} \dots q_r^{a_r}} \\ &= n^n. \end{aligned}$$

Hence

$$P_n = \prod_{d|q_1 q_2 \dots q_r} (b^{\frac{q_1 q_2 \dots q_r}{d}} - 1)^{\mu(d)}.$$

Since $\mu(d) = \pm 1$, it follows that P_n is the quotient of two polynomials in b with integral coefficients. The least exponent of b that appears in the numerator and in the denominator of the quotient is needed. Two separate cases will be considered, r even and r odd.

If r is even, then the least natural exponent of b in the numerator occurs when $d = q_1 q_2 \dots q_r$, and in this case the exponent of b is 1. Writing the numerator as the product of $(b-1)$ and a polynomial in b , it follows that all terms of the polynomial except the constant term, which is ± 1 , will have degree greater than 5. Then by expressing the numerator as one polynomial in b , all terms except the last two will be exactly divisible by b^2 , while the last two terms can be expressed as $\pm (b-1)$. Therefore, dividing the entire numerator by b^2 leaves a remainder of $b-1$ if the last two terms of the numerator are $\pm (b-1)$,

and $b^2 - b + 1$ if the last two terms are $-(b-1)$. In the denominator, however, since $q_1 < q_2 < \dots < q_r$, the least exponent is obtained for $d = q_2 q_3 \dots q_r$. Consequently, the exponent is equal to q_1 , therefore dividing the denominator by b^2 , a remainder of 1 or $b^2 - 1$ is obtained. But since $P_n = 1$ a contradiction results, because for $b > 2$ the numbers $b - 1$ and $b^2 - b > 1$ are always different from 1 and $b^2 - 1$.

If r is odd, then the least exponent of b in the numerator is obtained for $d = q_2 q_3 \dots q_r$; the least exponent of b in the denominator for $d = q_1 q_2 \dots q_r$, and as before a contradiction results.

The assumption: For every prime divisor p of $n^n - 1$, n belongs to an exponent less than n with respect to p , leads to a contradiction. Therefore it must be the case that $n^n - 1$ has at least one prime divisor p such that n belongs to the exponent n with respect to the modulus p . Since $(n, p) = 1$, Fermat's Theorem yields

$$n^{p-1} \equiv 1 \pmod{p}$$

whence by Theorem 5.6, $n \mid p - 1$, that is, $nk = p - 1$ for some natural number k , and $p = nk + 1$. So for every natural number $n > 1$, there exists at least one prime number of the form $nk + 1$ for some natural number k . From this and the remarks made at the beginning, the theorem follows.

There are several applications which follow from Theorems 5.7 and 5.8. One of these concerns the representations of the primes in base two.

Every prime number greater than 2 is odd, and hence the units digit of the prime in base two, with the exception of $2 = 10_{\text{two}}$ must have a units digit 1. Theorem 5.7 implies that for any natural number

m , there is a prime which, when represented in base two will have m zeros preceding the units digit 1. For example, 101, 101001, 10001, and 1100001, are primes expressed in base two with one, two, three and four zeros respectively, preceding the units digit 1. The proof follows from the fact that for any natural number m there is a prime p of the form $2^{m+1}k+1$, where k is a natural number. Therefore in the representation of this number in base two m of the last $m+1$ digits are zero, and one, the very last, is 1. If k is odd then exactly m of the digits preceding 1 are 0 while if k is even then the $m+1$ st digit preceding the 1 is also 0.

From Theorem 5.8 it can be deduced that there are infinitely many primes that are not elements of a triple of primes as discussed in Chapter IV. (See p. 34) That is, if from the set of primes one removes all those primes which belong to a triple of primes of the form $p, p+2, p+6$ or of the form $p, p+4, p+6$, then infinitely many primes still remain in the set. The proof follows.

From Theorem 5.8, there exist infinitely many prime numbers q of the form $15k+1$, where k is a natural number. For any of the q 's, it follows that $3|q+2$, $5|q+4$, $3|q-4$, and $5|q-6$. Since $q > 15$, it follows that $q+2$, $q+4$, $q-4$, and $q-6$ are all composite.

If q were any of the numbers of the first set then $q = p$, $q = p+2$, or $q = p+6$, and if these were prime, then in the first case $p+2 = q+2$ would be composite, in the second case $p+6 = q+4$ would be composite, and finally, in the third case the number $p = q-6$ would be composite. So none of the cases is possible.

Similarly, if the numbers $p, p+4, p+6$ are prime, then if

$p = q$, $p + 4 = q + 4$ is composite, if $q = p + 4$, then $p + 6 = q + 2$ is composite, and finally, if $q = p + 6$, then $p = q - 6$ is composite.

Thus it follows, in a sense, that there are not "too many" triples of primes of the form mentioned, since by removing all of them, there are still infinitely many primes remaining. This does not tell us that there is only a finite number of such triples of primes.

There are probably many other facts which can be established with the aid of the theorems of this chapter. Perhaps the reader will attempt to find and prove some of his own.

CHAPTER VI

DIRICHLET'S THEOREM

The methods that Dirichlet used to prove the theorem about primes in arithmetic progressions involve much more than the methods of elementary number theory. The methods are based upon the Riemann Zeta function and a special type of function called a character. The importance of the character lies in the fact that one may represent a sum over all natural numbers of a finite or infinite interval as the sum over the numbers of a particular arithmetic progression. The Riemann Zeta function is defined by a series and the importance of it arises in the properties of certain variations of the series.

In the discussion, the logarithms of complex numbers are used and for this reason Dirichlet's proof is called non-elementary. In 1949 Atle Selberg gave a different proof of the theorem. His proof does not involve logarithms of complex numbers and is referred to as the "elementary" proof. This does not mean that the new proof is simple since it is as difficult to understand as the original.

Since this paper is concerned primarily with number theory, the number-theoretic ideas and theorems that Dirichlet used will be discussed in detail, while the methods of analysis will be mentioned and the necessary theorems will be stated without proof. The interested reader may refer to LeVeque, Volume II, [12] for proofs which are not given.

Characters

A character is defined by the following:

Definition 6.1. A complex valued function, χ , defined on the natural numbers is called a character modulo k provided that:

- I. If $(a, k) > 1$, then $\chi(a) = 0$.
- II. $\chi(1) \neq 0$.
- III. For all a, b , $\chi(a \cdot b) = \chi(a) \chi(b)$.
- IV. If $a \equiv b \pmod{k}$, then $\chi(a) = \chi(b)$.

Those familiar with the elementary notions of group theory and congruence classes of integers will note that χ is a completely multiplicative function from the congruence classes of integers modulo k into the complex numbers. Hence χ is periodic with period k . From the definition several theorems are immediate.

Theorem 6.1. For every character χ , $\chi(1) = 1$.

Proof: By III, $\chi(1) = \chi(1 \cdot 1) = \chi(1) \chi(1)$ and so

$$\chi(1) [1 - \chi(1)] = 0,$$

and since $\chi(1) \neq 0$, $[1 - \chi(1)] = 0$ and $\chi(1) = 1$.

Theorem 6.2. If $(a, k) = 1$ and $\phi(k) = h$, then $(\chi(a))^h = 1$, that is, $\chi(a)$ is an h -th root of unity.

Proof: By Fermat's Theorem (Theorem 5.A),

$$a^h \equiv 1 \pmod{k}$$

and by III, IV, and Theorem 6.1,

$$(\chi(a))^h = \chi(a^h) = \chi(1) = 1.$$

With k given there always exists at least one character defined by:

$$\chi(a) = \begin{cases} 0 & \text{if } (a, k) > 1. \\ 1 & \text{if } (a, k) = 1. \end{cases}$$

That this function is indeed a character can be easily verified by checking I-IV of the definition.

Definition 6.2. The character defined above is called the principal character and is denoted by χ_0 .

The theorems and proofs which follow are, of necessity, somewhat technical and the reader interested only in the main result may skip to page 79 where the basic theorem on characters is given.

Theorem 6.3. For every natural number k , there exists a finite number of characters modulo k .

Proof: Let χ be a character modulo k . If $1 \leq a \leq k$, then $\chi(a)$ is 0 or an h -th root of unity, that is $\chi(a)$ must be chosen from a finite number of values. Since χ is periodic the value of $\chi(n)$ for any natural number n is determined since $n \equiv a \pmod{k}$ for some a where

$1 \leq a \leq k$. Since there is a finite number of a 's between 1 and k and a finite number of values that $\chi(a)$ can assume, there could not be an infinite number of χ 's.

It will be shown later that the number of χ 's is exactly equal to $\phi(k) = h$.

Theorem 6.4. If χ_1 and χ_2 are two characters modulo k , then $\chi_1\chi_2$ is also a character modulo k where $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$.

Proof: The proof follows directly from Definition 6.1.

Theorem 6.5. If χ is a character modulo k , then $\overline{\chi}$ is also a character,

where $\overline{\chi}(a) = \overline{\chi(a)}$.

Proof: I, II, and IV of Definition 6.1 are immediate. Since

$$\overline{\chi}(ab) = \overline{\chi(ab)} = \overline{\chi(a)\chi(b)} = \overline{\chi(a)} \overline{\chi(b)} = \overline{\chi}(a) \overline{\chi}(b), \text{ III also holds.}$$

Theorem 6.6. Let R_k denote a complete system of positive residues modulo k . Then

$$\sum_{a \in R_k} \chi(a) = \begin{cases} h & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$$

Proof: If $\chi = \chi_0$, then $\chi(a) = 1$ for each a in R_k where $(a, k) = 1$ and $\chi(a) = 0$ for each a in R_k where $(a, k) > 1$. Since $\phi(k) = h$, there are h a 's where $\chi(a) = 1$ and $k-h$ a 's where $\chi(a) = 0$, and so $\sum_{a \in R_k} \chi(a) = h$ if $\chi = \chi_0$. If R_k denotes a complete system of positive residues, then choose b such that $(b, k) = 1$, and $b > 1$. The set $bR_k = \{ba \mid a \in R_k\}$ is also a complete system of positive residues and since $\chi(a) = \chi(b)$ if $a \equiv b \pmod{k}$ it follows that

$$\sum_{a \in R_k} \chi(a) = \sum_{a \in R_k} \chi(ba) = \sum_{a \in R_k} \chi(a) \chi(b) = \chi(b) \sum_{a \in R_k} \chi(a).$$

and so $(1 - \chi(b)) \sum_{a \in R_k} \chi(a) = 0$, and since $\chi(b) \neq 1$ it follows that

$$\sum_{a \in R_k} \chi(a) = 0.$$

Theorem 6.3 verified that there can be only a finite number of characters modulo a fixed k , say c . The following theorem can now be proved:

Theorem 6.7. Let $G = \{\chi_0, \chi_1, \chi_2, \dots, \chi_{c-1}\}$ be the set of c characters for a fixed k . Then the set $G_i = \{\chi_i \chi_0, \chi_i \chi_1, \dots, \chi_i \chi_{c-1}\}$ is exactly the set G for each i where $0 \leq i \leq c$.

Proof: The theorem follows by showing that the c characters of G_i are distinct. That each element of G_i is indeed a character follows from Theorem 6.4.

Suppose $\chi_i \chi_m = \chi_i \chi_n$ for some i where $0 \leq i \leq c-1$, $0 \leq m \leq c-1$, $0 \leq n \leq c-1$, and $m \neq n$. Then for each a in R_k

$$\chi_i(a) \chi_m(a) = \chi_i(a) \chi_n(a).$$

If $(a, k) = 1$, then $\chi_i(a) \neq 0$ and by elementary algebra it follows that $\chi_m(a) = \chi_n(a)$; if $(a, k) > 1$, then $\chi_m(a) = 0 = \chi_n(a)$. Thus $\chi_m(a) = \chi_n(a)$ for every a in R_k . But this is impossible since the c characters in G are distinct. Hence $G = G_i$.

Before proving the next theorem two results from elementary number theory will be stated. The results are needed in the proof of the theorem. Proofs may be found in Landau. [9: 107-108]

Theorem 6.A. If $p > 2$ and $\ell > 2$, then there exists a number g such that g belongs to the exponent $\phi(p^\ell)$ modulo p^ℓ .

Theorem 6.B. If a is an odd number and $\ell > 2$, then

$$a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^\ell}$$

where $b \geq 0$ and b is some element of a particular residue class modulo $2^{\ell-2}$.

Theorem 6.8. If $d > 0$, $(d, k) = 1$ and $d \not\equiv 1 \pmod{k}$, then there is a character χ such that $\chi(d) \neq 1$.

Proof: Since $\chi(a) = 0$ for $(a, k) > 1$, it is sufficient to define the character for those a 's where $(a, k) = 1$ and verify II, III, and IV of the definition.

Since $d \not\equiv 1 \pmod{k}$ it follows that there is a prime p and an $\ell > 0$ such that $p^\ell | k$ and $d \not\equiv 1 \pmod{p^\ell}$. Two cases will be taken, $p = 2$ and $p > 2$.

Case I. Let $d \not\equiv 1 \pmod{p^\ell}$, $p > 2$, $\ell > 0$ and $p^\ell | k$; then $p \nmid d$ because $(d, k) = 1$. By Theorem 6.A there exists a g such that g belongs to the exponent $\phi(p^\ell)$ modulo p^ℓ , hence $g^1, g^2, g^3, \dots, g^{\phi(p^\ell)}$ form a reduced residue system modulo p^ℓ . For each a where $(a, k) = 1$, $p \nmid a$, thus there is a $b \geq 0$ such that $a \equiv g^b \pmod{p^\ell}$. Set

$$t = \exp\left(\frac{2\pi i}{\phi(p^\ell)}\right)$$

and define χ by $\chi(a) = t^b$. Then t^b has period $\phi(p^\ell)$ and b is uniquely determined modulo $\phi(p^\ell)$. Therefore χ is completely determined once g has been chosen. The second part of the definition is verified by $\chi(1) = t^0 = 1 \neq 0$. If $(a_1, k) = 1 = (a_2, k)$, $a_1 \equiv g^{b_1} \pmod{p^\ell}$ and $a_2 \equiv g^{b_2} \pmod{p^\ell}$, then $a_1 a_2 \equiv g^{b_1 + b_2} \pmod{p^\ell}$ and $\chi(a_1 a_2) = t^{b_1 + b_2} = \chi(a_1) \chi(a_2)$ and so the third part of the definition holds. The fourth follows from the fact that if $a_1 \equiv a_2 \pmod{k}$, then $a_1 \equiv a_2 \pmod{p^\ell}$ and if $a_1 \equiv g^{b_1} \pmod{p^\ell}$, $a_2 \equiv g^{b_2} \pmod{p^\ell}$, then $g^{b_1} \equiv g^{b_2} \pmod{p^\ell}$, and by a well-known theorem from elementary number theory it follows that $b_1 \equiv b_2 \pmod{\phi(p^\ell)}$. Hence

$$\chi(a_1) = t^{b_1} = \exp\left(\frac{2\pi i}{\phi(p^\ell)}\right)^{b_1} = \exp\left(\frac{2\pi i}{\phi(p^\ell)}\right)^{b_2} = t^{b_2} = \chi(a_2).$$

Now if d satisfies the hypothesis of the theorem then there exists an r such that

$$d \equiv g^r \pmod{p^\ell} \text{ and } \phi(p^\ell) \nmid r.$$

If $\phi(p^\ell) \mid r$, then let $\phi(p^\ell) \cdot m = r$. Then $d \equiv g^r \equiv (g^{\phi(p^\ell)})^m \equiv 1 \pmod{p^\ell}$ contradictory to the hypothesis. Therefore

$$\chi(d) = t^r = \exp\left(\frac{2\pi i}{\phi(p^\ell)}\right)^r \neq 1 \text{ since } \phi(p^\ell) \nmid r.$$

Case II. Let $d \not\equiv 1 \pmod{2^\ell}$, $\ell > 0$, $2^\ell \mid k$. Now $\ell > 1$, for if $\ell = 1$, then since k is even d must be odd and so $d \equiv 1 \pmod{2}$. Since 2 divides $d - 1$, 4 divides either $d - 1$ or $d + 1$. Each case will be considered separately.

Let 4 divide $d - 1$, that is $d \equiv 1 \pmod{4}$. Thus $\ell > 2$ and for $(a, k) = 1$ it follows from Theorem 6.B and the fact that $(a, 2) = 1$ that

$$a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^\ell} \text{ for } b \geq 0.$$

Let $t = \exp\left(\frac{2\pi i}{2^{\ell-2}}\right)$ and $\chi(a) = t^b$. Since t^b has period $2^{\ell-2}$ and b is determined modulo $2^{\ell-2}$, χ is well defined. We must verify that χ satisfies II, III, and IV of the definition. Since $\chi(1) = t^0 = 1$,

$\chi(1) \neq 0$. If $(a_1, k) = (a_2, k) = 1$, $a_1 \equiv (-1)^{\frac{a_1-1}{2}} 5^{b_1} \pmod{2^\ell}$ and

$a_2 \equiv (-1)^{\frac{a_2-1}{2}} 5^{b_2} \pmod{2^\ell}$, then

$$a_1 a_2 \equiv (-1)^{\frac{a_1-1}{2} + \frac{a_2-1}{2}} 5^{b_1+b_2} \equiv (-1)^{\frac{a_1 a_2 - 1}{2}} 5^{b_1+b_2} \pmod{2^\ell}$$

Hence $\chi(a_1 a_2) = t^{b_1+b_2} = t^{b_1} t^{b_2} = \chi(a_1) \chi(a_2)$. If $a_1 \equiv a_2 \pmod{k}$,

then $a_1 \equiv a_2 \pmod{p^\ell}$ and as before $\chi(a_1) = \chi(a_2)$.

Therefore if $d \equiv 1 \pmod{4}$, then $\frac{d-1}{2}$ is even and

$$d \equiv 5^r \pmod{2^\ell},$$

and since $0 < r < 2^{\ell-2}$, $2^{\ell-2} \nmid r$ and so

$$\chi(d) = t^r = \exp\left(\frac{2\pi i}{2^{\ell-2}}\right)^r \neq 1.$$

Let 4 divide $d+1$, that is $d \equiv -1 \pmod{4}$. With $(a, k) = 1$ and k even, a must be odd. Let

$$\chi(a) = (-1)^{\frac{a-1}{2}}.$$

Then $\chi(1) = (-1)^0 = 1 \neq 0$. If $(a_1, k) = (a_2, k) = 1$, then

$$\chi(a_1 a_2) = (-1)^{\frac{a_1 a_2 - 1}{2}} = (-1)^{\frac{a_1 - 1}{2}} (-1)^{\frac{a_2 - 1}{2}} = \chi(a_1) \chi(a_2).$$

If $a_1 \equiv a_2 \pmod{k}$, then since $4 \mid k$, it follows that a_1 and a_2 are either both odd or both even and so

$$\chi(a_1) = (-1)^{\frac{a_1 - 1}{2}} = (-1)^{\frac{a_2 - 1}{2}} = \chi(a_2)$$

Therefore χ is a character, $\frac{d-1}{2}$ is odd, and $\chi(d) = -1 \neq 1$, and the proof is complete.

Theorem 6.9. For fixed $a > 0$,

$$\sum_{\chi} \chi(a) = \begin{cases} c & \text{if } a \equiv 1 \pmod{k} \\ 0 & \text{otherwise.} \end{cases}$$

Proof: If $(a, k) > 1$, then $a \not\equiv 1 \pmod{k}$ and $\chi(a) = 0$ for each χ . If $(a, k) = 1$, and $a \not\equiv 1 \pmod{k}$, then $\chi(a) \neq 1$ for each χ and since there are c such χ 's, $\sum_{\chi} \chi(a) = 0$. If $(a, k) = 1$ and $a \equiv 1 \pmod{k}$, then there

exists a character χ_1 such that $\chi_1(a) \neq 1$, by Theorem 6.8. Then by Theorem 6.7

$$\sum_{\chi} \chi(a) = \sum_{\chi} \chi(a) \chi_1(a) = \chi_1(a) \sum_{\chi} \chi(a)$$

and so $\sum_{\chi} \chi(a) (\chi_1(a) - 1) = 0$, and since $\chi_1(a) \neq 1$ it follows that

$$\sum_{\chi} \chi(a) = 0.$$

Theorem 6.10. There are exactly $\phi(k) = h$ characters modulo k , that is $c = h$.

Proof: Let R_k denote a complete system of residues modulo k , and let G be the set of χ 's. Then

$$\sum_{a \in R_k} \sum_{\chi \in G} \chi(a) = \sum_{\chi \in G} \sum_{a \in R_k} \chi(a)$$

and since there is only one a in a complete residue system such that $a \equiv 1 \pmod{k}$ it follows that

$$\sum_{a \in R_k} \sum_{\chi \in G} \chi(a) = c + 0 + 0 + \cdots + 0 = c.$$

But by Theorem 6.6

$$\sum_{\chi \in G} \sum_{a \in R_k} \chi(a) = h + 0 + 0 + \cdots + 0 = h.$$

and so $c = h$.

Theorem 6.11. Let $b > 0$, $a > 0$, and $(b, k) = 1$. Then

$$\sum_{\chi} \frac{\chi(a)}{\chi(b)} = \begin{cases} h & \text{if } a \equiv b \pmod{k} \\ 0 & \text{otherwise.} \end{cases}$$

Proof: The congruence $bx \equiv 1 \pmod{k}$ has a solution which is unique modulo k . Let c be the solution; thus $bc \equiv 1 \pmod{k}$, and $(c, k) = 1$. then

$$\sum_{\chi} \frac{\chi(a)}{\chi(b)} = \sum_{\chi} \frac{\chi(a)\chi(c)}{\chi(b)\chi(c)} = \sum_{\chi} \frac{\chi(ac)}{\chi(bc)} = \sum_{\chi} \chi(ac)$$

Therefore

$$\sum_{\chi} \frac{\chi(a)}{\chi(b)} = \begin{cases} h & \text{if } ac \equiv 1 \pmod{k} \\ 0 & \text{otherwise} \end{cases}$$

but $ac \equiv 1 \pmod{k}$ if and only if $ac \equiv bc \pmod{k}$ which implies that $a \equiv b \pmod{k}$, since $(c, k) = 1$; and the theorem is proved.

The preceding theorem is the main one involving characters. As was mentioned before this theorem singles out the elements of a particular residue class modulo k and then by the relation

$$\sum_{\substack{u \leq a \leq v \\ a \equiv b \pmod{k}}} g(a) = \frac{1}{h} \cdot \sum_{u \leq a \leq v} g(a) \sum_{\chi} \frac{\chi(a)}{\chi(b)}$$

sums can be extended over infinite arithmetic progressions as well as over finite or infinite intervals.

L-Functions

Among the topics from analysis that are needed is the Riemann Zeta function. This function is defined by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

which is known to converge absolutely for $s > 1$. It is a special case of the Dirichlet's series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. The L-function, which is used in

the proof of the main theorem, is also a special case of the Dirichlet series and is defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where χ is a character modulo k . Since $|\chi(n)| = 1$ or 0 , the series

defined by the L-function also converges absolutely for $s > 1$. A fundamental relationship exists between the L-functions and the sequence of primes. This relationship is given in the following theorem.

Theorem 6.12. For $s > 1$, $L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$.

Proof: $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{\chi(n)}{n^s}$ and $\prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} =$

$\lim_{N \rightarrow \infty} \prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$ so it suffices to show that these two limits are

equal.

The series $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots = \sum_{n=0}^{\infty} x^n$ is known to converge for $|x| < 1$ and since $\left|\frac{\chi(p)}{p^s}\right| < 1$, it follows that $\prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} =$

$\prod_{p \leq N} \left(1 + \frac{\chi(p)}{p^s} + \frac{(\chi(p))^2}{p^{2s}} + \frac{(\chi(p))^3}{p^{3s}} + \dots\right)$. This last

product, upon expanding, contains terms of the form $\frac{\chi(n)}{n^s}$ where n is

the product of primes and powers of primes not exceeding N . Also each such n occurs exactly once because of unique factorization.

Since the series involved are absolutely convergent, the terms can be arranged in any order, that is:

$$(1) \quad \prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum' \frac{\chi(n)}{n^s}$$

where the accent indicates a summation, in the natural order, over all natural numbers n whose prime factorization includes only primes less than or equal to N . In particular, the sum contains all terms

$\frac{\chi(n)}{n^s}$ for which $n \leq N$. Therefore (1) can be written

$$\prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=1}^N \frac{\chi(n)}{n^s} + \sum'_{n > N} \frac{\chi(n)}{n^s}$$

where the primed sum is as before. But since $s > 1$,

$$0 < \sum'_{n > N} \frac{\chi(n)}{n^s} \leq \sum_{n=N+1}^{\infty} \frac{|\chi(n)|}{n^s} \leq \int_N^{\infty} \frac{|\chi(x)|}{x^s} dx = \frac{1}{(s-1)N^{s-1}} \quad \text{and so}$$

$$\lim_{N \rightarrow \infty} \sum'_{n > N} \frac{\chi(n)}{n^s} \leq \lim_{N \rightarrow \infty} \frac{1}{(s-1)N^{s-1}} = 0 \quad \text{and therefore:}$$

$$\lim_{N \rightarrow \infty} \prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{\chi(n)}{n^s} + \lim_{N \rightarrow \infty} \sum'_{n > N} \frac{\chi(n)}{n^s} =$$

$$\lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{\chi(n)}{n^s}.$$

Using Theorem 6.12 and by letting $\chi = \chi_0$ it follows that

$$\begin{aligned} L(s, \chi_0) &= \prod_{p|k} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p|k} (1 - p^{-s})^{-1}, \quad \text{and so } L(s, \chi_0) = \\ &= \prod_{p|k} (1 - p^{-s})^{-1} \cdot \frac{\prod_{p|k} (1 - p^{-s})^{-1}}{\prod_{p|k} (1 - p^{-s})^{-1}} = \frac{\prod_{p|k} (1 - p^{-s})^{-1}}{\prod_{p|k} (1 - p^{-s})^{-1}} = \frac{\zeta(s)}{\prod_{p|k} (1 - p^{-s})^{-1}} = \\ &= \prod_{p|k} (1 - p^{-s}) \zeta(s). \end{aligned}$$

The behavior of $\zeta(s)$ in the neighborhood of 1 must be investigated.

The following theorems are needed and are stated without proof.

Proofs can be found in LeVeque, Volume II. [12]

Theorem 6.13. $\lim_{s \rightarrow 1^+} \zeta(s)(s-1) = 1$ and $\lim_{s \rightarrow 1^+} \zeta(s) = \infty$

Theorem 6.14. $L(s, \chi_0)$ is continuous for $s > 1$ and

$$\lim_{s \rightarrow 1^+} (s-1)L(s, \chi_0) = \frac{h}{k}, \text{ where } h = \phi(k).$$

Theorem 6.15. For $\chi \neq \chi_0$, $L(s, \chi)$ converges.

Theorem 6.16. If $\chi \neq \chi_0$, then $L(s, \chi)$ has a continuous derivative for $s > 0$, and is therefore itself continuous.

Theorem 6.17. For each χ the function

$$F(s, \chi) = \log L(s, \chi) - \sum_p \frac{\chi(p)}{p^s}$$

is bounded in absolute value for $s > 1$.

Theorem 6.18. For any χ , $L(1, \chi) \neq 0$.

The most difficult proof of the theorems stated is the one that $L(1, \chi) \neq 0$. Dirichlet proved the theorem, as does LeVeque, in two cases. The first case is for those χ which assume at least one non-real value, and the second for those χ which have only real values, that is $\chi(a) = \pm 1$ for each a where $(a, k) = 1$. It is somewhat surprising that in the latter case the proof is the more difficult.

With the preceding background information, Dirichlet's Theorem can now be proved.

Theorem 6.19. Dirichlet's Theorem. If $(k, b) = 1$, then there are infinitely many primes p in the progression $kt + b$ ($t = 0, 1, 2, 3, \dots$).

Proof: First note that the statement is equivalent to the statement that there are infinitely many primes p such that $p \equiv b \pmod{k}$.

From Theorem 6.17

$$\log L(s, \chi) = F(s, \chi) + \sum_p \frac{\chi(p)}{p^s}$$

and multiplying both sides of the equality by $\frac{1}{\chi(b)}$ and summing over all χ , where χ is taken modulo k we obtain

$$\sum_{\chi} \frac{\log L(s, \chi)}{\chi(b)} = \sum_{\chi} \frac{F(s, \chi)}{\chi(b)} + \sum_{\chi} \sum_p \frac{\chi(p)}{\chi(b)} =$$

$$\sum_{\chi} \frac{F(s, \chi)}{\chi(b)} + \sum_p \frac{1}{p^s} \sum_{\chi} \frac{\chi(p)}{\chi(b)}$$

and then by Theorem 6.11, which gives $\sum_{\chi} \frac{\chi(p)}{\chi(b)} = h$ if $p \equiv b \pmod{k}$ and 0 otherwise it follows that

$$(2) \quad \sum_{\chi} \frac{\log L(s, \chi)}{\chi(b)} = \sum_{\chi} \frac{F(s, \chi)}{\chi(b)} + h \sum_{p \equiv b \pmod{k}} \frac{1}{p^s}.$$

Consider the limit as s approaches 1 from the right of each side of (2). The first term on the right remains bounded by Theorem 6.17. We need to show that the left side becomes infinite and then the second term on the right, $h \sum_{p \equiv b \pmod{k}} \frac{1}{p^s}$ will also tend to infinity. This can happen only if there is an infinite number of primes p such that $p \equiv b \pmod{k}$. For suppose there were only a finite number of primes in the progression. Then summing this finite number of terms would certainly yield a finite sum and since h is fixed the expression

$$h \sum_{p \equiv b \pmod{k}} \frac{1}{p^s}$$

would be finite. We show, therefore, that the left side tends to infinity as s approaches 1 from the right.

By Theorem 6.12.

$$\lim_{s \rightarrow 1^+} L(s, \chi_0) = \lim_{s \rightarrow 1^+} \prod_{p|k} (1 - p^{-s}) \zeta(s) = \infty,$$

and so $\lim_{s \rightarrow 1^+} \frac{\log L(s, \chi_0)}{\chi_0(b)} = \infty$. Now for $\chi \neq \chi_0$, $L(s, \chi)$ is continuous

at $s = 1$, and so

$$\lim_{s \rightarrow 1^+} \frac{\log L(s, \chi)}{\chi(b)} = \frac{\log L(1, \chi)}{\chi(b)}$$

which exists and is finite since $L(1, \chi) \neq 0$, and $L(s, \chi)$ converges for $\chi \neq \chi_0$. Therefore,

$$\left| \lim_{s \rightarrow 1^+} \sum_{\chi \neq \chi_0} \frac{\log L(s, \chi)}{\chi(b)} \right| < \infty$$

and the left side of (2) tends to infinity as s approaches 1 from the right.

CHAPTER VII

SUMMARY AND EDUCATIONAL IMPLICATIONS

In this paper the material concerning primes in arithmetic progressions is discussed. This presentation makes the research concerning this topic more readable and more readily available to the student of elementary number theory. It also provides examples of how the basic theorems of number theory can be used to prove theorems about primes in arithmetic progressions.

Summary

In Chapter I the statement of the problem, scope of the paper, methods and procedures, and expected outcomes are given. Chapter II includes a very elementary introduction to the meaning of Dirichlet's Theorem. In Chapter III a discussion of arithmetic progressions in which each term is prime is presented. The basic result is Theorem 3.7, which states that if n odd prime terms are in an arithmetic progression, then the common difference is divisible by each prime less than n . Chapter IV provides generalizations of the problems concerning arithmetic progressions in which each term is prime. Prime twin pairs and quadruplets are discussed and a presentation of a recent conjecture known as Conjecture H is given. This conjecture, if proven, would provide answers to many of the unanswered questions of ele-

mentary number theory. Chapter V is devoted to proofs of special cases of Dirichlet's Theorem. It is shown how the well-known results of elementary number theory can be used to prove special cases. In Chapter VI an outline of Dirichlet's general theorem is given. The proofs of the necessary theorems involving number-theoretic ideas are given while the theorems involving complex analysis are stated without proof.

Educational Implications

Many of the ideas of mathematics, and number theory in particular, can be understood by the layman and also by secondary school students. It is important that some of these ideas be presented to these groups in a systematic manner. A study such as this one, in addition to consolidating the research, presents the necessary background needed for an understanding of the problem, and brings the collection of knowledge to many students.

As a result of reading this thesis, the student should gain an awareness of some of the elementary ideas of number theory and of the current and past research that has been done in the area concerning primes in arithmetic progressions. It is also of significance that the reader, who is a potential teacher at either the public school or the college level, may find motivation material for his class, and perhaps enlarge on some of the ideas presented.

Undoubtedly the most significant result of this paper lies in the experience that the investigator gained in its preparation.

A SELECTED BIBLIOGRAPHY

- (1) Ayoub, Raymond, An Introduction to the Theory of Numbers, Providence, R.I.: American Mathematical Society, 1963.
- (2) Bateman, P. T., and Low, M., "Prime Numbers in Arithmetic Progressions with Difference 24," The American Mathematical Monthly, Vol. 72 (1965), pp. 139-143.
- (3) Butler, George, Some Results Concerning the Distribution of the Prime Numbers, (unpub. M.S. thesis, Oklahoma State University, 1963).
- (4) Davenport, H., The Higher Arithmetic, An Introduction to the Theory of Numbers, London; Hutchinson's University Library, 1952.
- (5) Dickson, Leonard E., History of the Theory of Numbers, Washington, Carnegie Institute, Vol. I, II, III, 1919.
- (6) Easterman, T., Introduction to Modern Prime Number Theory, Cambridge, England, Cambridge University Press, 1952.
- (7) Frankel, Abraham A., Integers and Theory of Numbers, New York; Scripta Mathematica, Yeshiva University Press, 1955.
- (8) Hardy, G. H., "An Introduction to the Theory of Numbers," Bulletin American Mathematical Society, Vol. 35 (1929), p. 818.
- (9) Hardy, G. H. and Littlewood, E. J., "Some Problems of Partitio Numerorum III, Acta Mathematica, Vol. 44 (1923), pp. 1-70.
- (10) Landau, Edmond, Elementary Number Theory, New York: Chelsea Pub. Co., 1958.
- (11) Lehmer, D. H. Tables Concerning the Distribution of Primes up to 37 Million, Deposited in UMT File, Reviewed in Math Tables and Aids to Computation, Vol. 13 (1959), pp. 56-57.
- (12) LeVeque, William J., Topics in Number Theory, Reading Mass.: Addison Wesley Pub. Co. Inc., Vol. I, II, 1956.

- (13) Long, Calvin T., Elementary Introduction to Number Theory, Boston: D. C. Heath and Co., 1965.
- (14) Martin, Atrebas, "Prime Numbers in Arithmetical Progressions," School Science and Mathematics, Vol. 13 (1913), pp. 793-797.
- (15) Mathematical Association of America, Course Guide for the Training of Junior High and Senior High Mathematics Teachers, 1961.
- (16) _____, Course Guide for the Training of Teachers of Elementary School Mathematics, 1964.
- (17) Polya, G., "Heuristic Reasoning in the Theory of Numbers," American Mathematical Monthly, Vol. 66 (1959), pp. 375-384.
- (18) Popovici, Constantin P., "Sur le theoreme de Dirichlet relatif a L'infinite des nombres premiers positifs de la forme $4k+1$ et $6k+1$," Academia Republicii Populare Romine Comunicarile Bucharest, Vol. II (1961), pp. 767-772.
- (19) Rotkiewicz, A. "Demonstration Arithmetique de L'existence D'une Infinite de Nombres Premiers de la forme $nk+1$," L'enseignement Mathematique, Vol. 7 (1962), pp. 277-280.
- (20) Schnizel, A. and Sierpinski, W. "Sur Certaines Hypotheses concernant les Nombres Premiers," Acta Arithmetica, Vol. 4 (1958), pp. 185-208 and Corrigendum, Vol. 6 (1960), p. 259.
- (21) Selberg, A. "An Elementary Proof of Dirichlet's Theorem About Primes in Arithmetic Progressions," Annals of Mathematics, Vol. 50 (1949), pp. 297-313.
- (22) Selmer, E. S., "A Special Summation in the Theory of Prime Numbers and its Application to Bruns Sum," Norsk Math. Tidsskr, Vol. 24 (1942), pp. 74-81.
- (23) Shanks, Daniel, Solved and Unsolved Problems in Number Theory, Washington: Spartan Books, Vol. I, 1962.
- (24) Sierpiński, W. A Selection of Problems in the Theory of Numbers, New York: MacMillon, 1964.
- (25) _____, Elementary Theory of Numbers, Warszawa, Poland: Panstwowe Wydawnictwo Naukowe, 1965.
- (26) _____, "Sur Quelques Consequences D'une Hypothese de M. A. Schinzel," Bulletin Royale Sciences Liege, Vol. 31 (1962), pp. 317-320.

- (27) Thebault, Victor. "Sur Les Nombres Premiers Impairs,"
C. R. Academie Sci. Paris, Vol. 218 (1944), pp. 223-224.
- (28) Tietze, Heinrich. Famous Problems of Mathematics, New York:
Graylock Press, 1965.

VITA

Melvin Robert Woodard

Candidate for the Degree of

Doctor of Education

Thesis: PRIMES IN ARITHMETIC PROGRESSIONS

Major Field: Higher Education (Mathematics)

Biographical:

Personal Data: Born near Bentley Creek, Pennsylvania, February 25, 1936, the son of Harold Charles and Mary Lytle Woodard.

Education: Attended Bentley Creek grade school in Bradford County, Pennsylvania; graduated from Troy High School, Troy, Pennsylvania, in 1954; received the Bachelor of Science degree from Mansfield State College, Mansfield, Pennsylvania in 1958 with a major in Education (Mathematics); attended Syracuse University, Syracuse, New York, in the summer of 1959, Montclair State College, Upper Montclair, New Jersey, during the summer of 1961, and the University of Illinois during the academic year 1961-1962 and summer of 1962; received the Master of Arts degree from the University of Illinois in August, 1962, with a major in Mathematics; completed requirements for the Doctor of Education degree at Oklahoma State University, Stillwater, Oklahoma, in July, 1966.

Professional experience: Taught mathematics at Horseheads Junior High School, Horseheads, New York, 1958-1961; was an assistant professor of mathematics at Indiana State College, Indiana, Pennsylvania, 1962-1964; was a graduate assistant in mathematics at Oklahoma State University during the summer of 1965, and an instructor in education during the 1965-1966 academic year.

Organizations: Member of Mathematics Association of America, National Council of Teachers of Mathematics, National Education Association, and Phi Delta Kappa.