FUNDAMENTAL THEOREMS
ON THE DISTRIBUTION OF PRIME NUMBERS

by 1264

ROBERT T. CURRY
B. S., Kansas State University, 1966

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements of the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan,Kansas

1970

Approved by:

Eckford Cohen
Major Professor

TABLE OF CONTENTS

INTRODUCTION

"I have sometimes thought that the profound mystery which envelops our conceptions relative to prime numbers depends upon the limitations of our faculties in regard to time, which like space may be in its essence poly-dimensional, and that this and such sort of truths would become self evident to a being whose mode of perception is according to superficially as distinguished from our own limitation to linearly extended time."

J. J. Sylvester

The theory of numbers is one of the oldest of the presently "respectable" mathematical disciplines, and the study of prime numbers one of its fundamental topics. While this paper culminates with Viggo Brun's theorem on the convergence of the harmonic series of the twin primes, the major portion is dedicated to a systematic development of the fundamental theorems which lead to this important result.

As might be expected, the paper begins with Euclid's theorem on the number of primes and then proceeds to a study of the harmonic series of primes. The major result here is Euler's theorem which proves that this so-called Euler series is divergent. Also developed are two O-estimates (see Appendix) of its partial sums. One,

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log x,$$

is obtained from Legendre's theorem, $\pi(x) = o(x)$ as $x \to \infty$. (Theorem 6)

The other,

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + C + 0\left(\frac{1}{\log x}\right) \quad \text{for } x \geq 2$$

is derived from Chebyshev's theorem, $\pi(x) = 0 \frac{x}{(\log x)}$. (Theorem 10)

The Legendre and Chebyshev theorems are developed in turn from earlier estimates of the arithmetic function $\pi(x)$, which represents the number of positive primes $p \leq x$ where x is some real number.

Analogously, Brun's theorem is obtained from an estimate of the function

$$T * (x) < Cx \left(\frac{\log \log x}{\log x}\right)^2 \quad \text{for } x > 3$$

where $T * (x)$ represents the number of twin primes not exceeding x, and C is a positive constant.

It will be noted that a theorem concerning the number of twin primes is conspicuously absent, since it has yet to be shown if their number is infinite. (According to Landau, "One would certainly place one's bet on a 'yes' answer").

ELEMENTARY METHODS

In this section we look at several proofs of Euclid's theorem dealing with the fact that there are an infinite number of primes. A second theorem -- usually called Euler's theorem -- demonstrates that the harmonic series of the prime numbers is divergent, which is a much stronger result, and proves Euclid's theorem as a corollary.

Let us consider first the simplest and earliest proof of Euclid's theorem: Euclid's own.

THEOREM 1.a: There exist an infinite number of primes.

Proof: Suppose there exist only k primes

$$2, 3, 5, \ldots, p_k,$$

and consider the number

$$(2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_k) + 1.$$

This number is certainly not divisible by any of the k primes, for such a supposition would lead immediately to the conclusion that 1 was also divisible by that prime. Hence the number is either itself a prime or is divisible by some prime which is larger that p_k -- either of which results lead to a contradiction of the original assumption, thus proving the theorem.

The second proof -- due to Polya -- depends on the fact that the Fermat numbers are relatively prime in pairs. The Fermat numbers are, of course, numbers of the form

$$F_n = 2^{2n} + 1.$$

The following preliminary is necessary.

<u>LEMMA 1</u>: No two distinct Fermat numbers have a common divisor greater than 1.

<u>Proof</u>: Consider F_n and F_{n+k}, where $k > 0$. Suppose the following is true.

$$m|F_n \quad \text{and} \quad m|F_{n+k}$$

Then if we let $x = 2^{2n}$, we see that

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2n+k} - 1}{2^{2n} + 1}$$

$$= \frac{(2^{2n})^{2k} - 1}{2^{2n} + 1}$$

$$= \frac{x^{2k} - 1}{x + 1}$$

$$= x^{2k} - 1 - x^{2k-2} + \ldots -1$$

Therefore $F_n|(F_{n+k} - 2)$ and hence

$$m|F_{n+k} \quad \text{and} \quad m|(F_{n+k} - 2)$$

which implies that $m|2$. However, since F_{n+k} is odd, it follows that $m - 1$.

The proof of Euclid's theorem now follows very easily.

<u>THEOREM 1.b</u>: There exist an infinite number of primes.

<u>Proof</u>: Since each of the numbers $F_1, F_2, \ldots, F_n$ is divisible by an odd prime (perhaps the number itself) which does not divide any of the others, it follows that there are at least n odd primes which do not exceed F_n. Thus, since the result holds for all n, the number of primes must be infinite.

Euclid's theorem can be proved in a stronger form by noting that every integer is representable as the product of a square and a square-free number.

Definition: An integer is said to be square-free if the multiplicities of the primes in its standard factorization dc not exceed one.

LEMMA 2: Every integer $n \geq 1$ can be expressed as the product of a square and a square-free number.

Proof: Recalling the fundamental theorem of arithmetic, we can represent n as follows:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

Now every exponent is either of the form 2k or 2k + 1. Thus, (reindexing if necessary)

$$n = p_1^{2k_1} p_2^{2k_2} \cdots p_j^{2k_j} p_{j+1}^{2k_{j+1}+1} \cdots p_n^{2k_n +1}$$

$$= p_1^{2k_1} \cdots p_n^{2k_n} p_{j+1} \cdots p_n$$

$$= (p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n})^2 (p_{j+1} p_{j+2} \cdots p_n)$$

THEOREM 2: $\pi(n) \geq A \log n$, where $\pi(n)$ represents the number of primes not exceeding n, and where A is a positive constant.

Proof: Let $p_1, p_2, \ldots, p_r$ be the primes less than or equal to n, i.e., $r = \pi(n)$. By lemma 2 we can write

$$n = (n_1)^2 m$$

where m is square-free. Since the square-free integers are composed of primes which appear only to the first power, the number of square-free integers $\leq n$ does not exceed

$$\binom{r}{0} + \binom{r}{1} + \ldots + \binom{r}{r} = 2^r .$$