ON THE EXISTENCE OF PRIME NUMBERS IN POLYNOMIAL SEQUENCES, AND ODD PERFECT NUMBERS

.

.

.

.

BY

.

ACQUAAH PETER
(ID: 10191563)

.

.

.

.

A THESIS PRESENTED TO THE DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DOCTOR OF PHILOSOPHY IN MATHEMATICS.

.

.

.

.

UNIVERSITY OF GHANA, LEGON

JULY 2015

DECLARATION

This work was carried out in the University of Ghana, Legon in partial fulfillment of the requirement for the degree of Doctor of Philosophy at the University of Ghana, Legon. I hereby declare that except where due acknowledgment is made; this work has never been presented wholly or partially in part for the award of a degree in this or any other University.

. Student: Acquaah Peter.....

. Supervisor: Dr. Margaret McIntyre.....

. Co-supervisor: Dr. Adu-Gyamfi Douglas.....

ACKNOWLEDGEMENTS

I thank my Lord, Jesus Christ, for letting me through all the difficulties; allowing me to complete my research.

I would like to express my special appreciation and thanks to my advisors Dr. Margaret McIntyre and Dr. Douglas Adu-Gyamfi . Thank you for encouraging my research and your advice have been invaluable.

I am grateful to Dr. Maciej Dunajski MARM (Mentoring African Research in Mathematics scheme) mentor, and the London Mathematical Society for giving me the opportunity to complete my work successfully.

This research has been supported by the University of Ghana-Carnegie Next Generation of Academics in Africa project with funding from the Carnegie Corporation of New York. Without your support it would have been difficult to carry out this research in Ghana.

Finally, I say thank you to my colleagues Emmanuel Djabang, Eyram Schwinger, John De-Graft Mensah, Peace Ogbogbo, Prince Osei Koree, Thomas Katsekpor, Vasco Normenyo, Anton Asare-Tuah, Ralph Twum, for your support.

DEDICATION

I dedicate my dissertation to my family and friends. A special feeling of gratitude goes to Rebecca Aba Acquaah, Samuel Acquaah, Florence Acquaah and Abena Acquaah. I also dedicate this dissertation to the Mathematics Department of the University of Ghana.

ABSTRACT

It is known that certain polynomials of degree one, with integer coefficients, admit infinitely-many primes. In this thesis, we provide an alternative proof of Dirichlets theorem concerning primes in arithmetic progressions, without applying methods involving Dirichlet characters or the Riemann Zeta function. A more general result concerning multiples of primes in short-intervals is also provided.

This thesis also considers problems concerning the existence of odd perfect numbers. The main contribution is a good upper-bound on the largest prime divisor of an odd perfect number. In addition, we show how new results concerning odd perfect numbers or k - perfect numbers can be obtained by applying a property of completely-multiplicative functions.

Contents

Chapter 1

Introduction

1.1 Scope of the thesis

This study is concerned with two important research areas in number theory: the existence of odd perfect numbers and the existence of prime numbers in short intervals and polynomial sequences.

Even though advanced tools like complex analysis, ergodic theory and the theory of harmonics are generally used in the study of the distribution of prime numbers , we focus on the elementary methods of sieve theory to prove our results. Generally, the study of odd perfect numbers do not involve advanced tools from analysis and so the subject is a little isolated from most number theory discussions. By considering special completely-multiplicative functions, we derive new necessary conditions for the existence of an odd perfect number(OPN).

For most of the standard definitions, theorems and proofs, we follow the styles of the following books, notes and papers: Wissam Raji [54, Chapters, 2,4,7 and 8], Yinim Ge [56], Chen [11], Apostol [3, Chapters, 2,3,4,7,11,12 and 13], Dickson [13] and Apostol [4].

1.2 Goals of the thesis

We investigate some problems related to the distribution of prime numbers in short-intervals and polynomial sequences. We also consider questions about the existence of odd perfect numbers. The main goals of the thesis can be summarized as follows:

(i) **Establish alternative proofs of results about prime numbers in intervals of the form** $[kx, (k+j)\,x]; x, k, j \in \mathbb{R}^+$**.**

It is known that there is always a prime in the intervals $[x, 2x]$, $[2x, 3x]$ and $[3x, 4x], x \geq 1$. The proofs we provide in this thesis are based on inequalities involving the prime number counting function.

(ii) **Establish an alternative proof of Dirichlet's theorem concerning prime numbers in arithmetic progressions.**

Dirichlet provided a sufficient condition for an arithmetic progression of the form $an + b, a, b \in \mathbb{N}, n \in \mathbb{Z}$ to admit infinitely many prime numbers. His method relied heavily on techniques from complex analysis. We provide an alternative proof without resorting to properties of the Riemann-Zeta function.

(iii) **Investigate properties of** $\lambda-$**stationary polynomials**

Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients. For each $\lambda > 0, z \in \mathbb{Z}$ and $f \in \mathbb{Z}[x]$; consider the sequence

$$T_f^{\lambda}(z) = \left(a_f^{\lambda}(z, n)\right)_{n \geq 0}$$

defined in Chapter 3. We say the sequence $T_f^{\lambda}(z)$ is *stationary* if there exist positive integers m and u such that for every $n \geq m$, $a_f^{\lambda}(z, n) \leq u$; This says, $T_f^{\lambda}(z)$ is bounded above. Furthermore, f is said to be $\lambda-$ *stationary* if for every integer z, the sequence $T_f^{\lambda}(z)$ is stationary. We find that many number theoretical problems can be formulated using $\lambda-$ stationary polynomials in $\mathbb{Z}[x]$.

(iv) **Establish a result that determines a 'good' upper-bound for the largest prime divisor of an odd perfect number.**

Most results concerning an OPN, x, are of the form; x has a prime divisor greater than n, where n is some given constant. We give a result that connects the largest prime divisor of an OPN x to the number itself.

(v) **Provide necessary conditions for a positive integer to be an OPN.**

We use a simple result about completely multiplicative functions to establish new necessary conditions that an OPN must satisfy. It is clear that the technique can be used to elaborate further conditions which OPN's must satisfy(by using different completely multiplicative functions) so here we confine ourselves to two results.

1.3 Summary of key results

1.3.1 On OPNs

By definition, a positive integer x is *perfect* if

$$\sum_{d|x} d = 2x.$$

The following result bounds the largest prime divisor, p, of an OPN x as a function of x.

Proposition 1 *(Acquaah P., Konyagin S.[2]) The largest prime divisor of an odd perfect number g is less than $(3g)^{1/3}$.*

This statement improved the following results.

Proposition 2 *(Acquaah P. [1]) The largest prime divisor of an odd perfect number g is less than $g^{1/2}$.*

Proposition 3 *If g is an odd perfect number and p^u is a prime power divisor of g then $p^u < \sqrt{g}$.*

It is known that if N is an OPN then it can be expressed in the form

$$N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$$

where $p \equiv \alpha \equiv 1 \pmod 4$, p a prime, $p^{\alpha} || N$ and $q_1, q_2, ..., q_k$ are distinct primes. We apply a key property of completely multiplicative functions to derive the following results.

Proposition 4 *If $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN and $5|N$ then either (i) $p \equiv 1$ or $9 \pmod{10}$ or (ii) $q_i \equiv 1 \pmod{10}$ and $r_i = 5m + 2$ for some $m \geq 0, i\, (1 \leq i \leq k)$.*

Proposition 5 *If $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN then $T \equiv 0$ or $1 \pmod 4$ where T is the cardinality of*

$$|\{i | 1 \leq i \leq k, r_i \text{ odd}, q_i \equiv 1 \pmod 4\}|.$$

1.3.2 On Prime numbers in polynomial sequences or short intervals

We begin with the proposition that will serve as an important tool in most of our proofs, especially the alternative proof of Dirichlet's theorem. This is proved in chapter 3, section 2.

Proposition 6 *Let $a \in \mathbb{N}, k \in \mathbb{N}, a_k = (a, a+1, ..., a+k-1)$ and $A = \{p_1, p_2, ..., p_n\}$, a finite set of primes. Then the number of components of a_k that are divisible by some prime in A is less than or equal to*

$$\sum_{\substack{d | p_1 p_2 ... p_n \\ d > 1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor + n$$

where $\omega(d)$ is the number of distinct prime divisors of d and μ is the Moebius function.

The importance of this proposition is easy to see. For if $D = (1, 2, 3, ..., k)$ (the special case) then the number of components of D that are divisible by some prime in A is equal to

$$\sum_{\substack{d|p_1p_2...p_n \\ d>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

Therefore, the number of primes numbers in A plays a very important role in the general case $a_k = (a, a+1, ..., a+k-1)$. We provide alternative proofs of the following statements:

Proposition 7 *For $n > 2, n \in \mathbb{N}$, there exist primes p_1, p_2 and p_3 such that $n < p_1 < 2n, 2n < p_2 < 3n$ and $3n < p_3 < 4n$.*

Proposition 8 *If $a, b \in \mathbb{N}, \gcd(a, b) = 1$ then there are infinitely-many primes of the form $an + b$.*

1.4 Structure of the thesis

The thesis consists of six main chapters as follows:

Chapter 1: Introduction

Chapter 1, the current chapter, provides a summary of the content of the thesis.

Chapter 2: Introduction(Prime numbers)

This chapter, gives a summary of some important mathematical ideas used in the study of the distribution of prime numbers, especially those that are relevant to our discussion. We also give a sketch of Dirichlet's proof concerning the distribution of prime numbers. Furthermore, a summary of results concerning the distribution of prime numbers in short intervals or polynomials is provided.

Chapter 3: Main results (Prime numbers)

This chapter consists of new results and alternative proofs of some known results. The key ingredient in most of the proofs in this chapter is proposition

6. The general idea is to provide proofs that use only elementary ideas.

Chapter 4: Introduction(OPNs)

This chapter, gives a summary of important mathematical ideas used in the study of OPNs, especially those that are relevant to our discussion.

Chapter 5: Main results (OPNs)

This chapter consists of new results and alternative proofs of some known results. The key ingredient in most of the proofs in this chapter is a property of completely multiplicative functions.

Chapter 6: Summary and Conclusion

In this chapter, we will provide a brief summary of the ideas covered in the thesis. Possible future directions concerning problems that are related but could not be answered in this work will also be considered.

Chapter 2

Introduction(Prime numbers)

2.1 Arithmetic functions & the Fundamental Theorem of Arithmetic

A positive integer p is prime if $p \neq 1$ and the only positive divisors of p are 1 and p. Prime numbers are important to mathematicians and in particular number theorists because of the *Fundamental Theorem of Arithmetic* [31].

Theorem 9 *Every positive integer n can be written in the form*

$$n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \tag{2.1}$$

where $p_1, p_2, ..., p_k$ are distinct primes and $r_1, ..., r_k$ are positive integers. The product $p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ is unique up to the ordering of the prime-powers $p_1^{r_1}, p_2^{r_2}, ..., p_k^{r_k}$.

It is generally accepted that primes are the atoms of positive integers that are greater than 1. This does not mean that, given a positive integer greater than 1, we can efficiently factorize it into a product of prime powers. We have no closed form to generate all of the prime numbers even though we know that there are infinitely-many of them, a result for which there are many different proofs. The reader is referred to [28,30,15,24] for different proofs of the infinitude of primes.

Definition 1: An *arithmetic function* is any function of the form $f : \mathbb{N} \longrightarrow \mathbb{C}$. Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be an arithmetic function. f is:
(i) *multiplicative* if for every $a, b \in \mathbb{N}$;

$$f(ab) = f(a) f(b)$$

whenever $\gcd(a, b) = 1$;
(ii) *completely multiplicative* if for every $a, b \in \mathbb{N}; f(ab) = f(a) f(b)$. The following statement is a characterization of arithmetic functions.

Theorem 10 *Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be an arithmetic function not identically zero, that is $f \neq 0$. f is multiplicative if and only if*

$$f(1) = 1 \text{ and } f(n) = \prod_{p^\alpha || n} f(p^\alpha) \qquad (n \in \mathbb{N}), \tag{2.2}$$

where $p^\alpha || n$ means that p^α is an exact power of p dividing n. Furthermore, if f is a completely multiplicative function then

$$f(p^\alpha) = (f(p))^\alpha$$

for every prime-power p^α.

Therefore, if an arithmetic function is not identically zero then it is uniquely-determined by its value on prime powers. In (2.2), what happens if $n = 1$? By convention, we write

$$\prod_{a \in \varnothing} f(a) = 1$$

and

$$\sum_{a \in \varnothing} f(a) = 0$$

for an arithmetic function f. Therefore, in (2.2), if $n = 1$, we have

$$f(1) = \prod_{p^\alpha || 1} f(p^\alpha) = \prod_{a \in \varnothing} f(a) = 1.$$

Example 1:

(a) **(sum of the kth powers of the positive divisors of n).**

For $k \in \mathbb{N} \cup \{0\}, n \in \mathbb{N}$;

$$\sigma_k(n) = \sum_{d|n} d^k.$$

In particular, set $\sigma_1(n) = \sigma(n)$ and $\sigma_0(n) = \tau(n)$ where

$$\tau(n) = \sum_{t|n} 1.$$

Let $n \in \mathbb{N}$, the *sum of the divisors* of n is given by $\sigma(n) = \sum_{t|n} t$. We have (i) σ_k is multiplicative but not completely-multiplicative. To see multiplicativity of σ_k; let $a, b, k \in \mathbb{N}, \gcd(a,b) = 1$ then

$$\sigma_k(ab) = \sum_{d|ab} d^k = \sum_{d_1|a, d_2|b} d_1^k d_2^k = \sum_{d_1|a} d_1^k \sum_{d_2|a} d_2^k = \sigma_k(a)\sigma_k(b).$$

To show that σ_k is not completely-multiplicative, let $n = 12 = 2^2.3, m = 4 = 2^2$. Then

$$\begin{aligned} \sigma_k(2^2) &= \frac{2^{3k}-1}{2^k-1}, \sigma_k(3) = \frac{3^{2k}-1}{3^k-1}. \\ \text{So, } \sigma_k(n) &= \frac{2^{3k}-1}{2^k-1}.\frac{3^{2k}-1}{3^k-1}, \sigma_k(m) = \frac{2^{3k}-1}{2^k-1} \text{ and} \\ \sigma_k(n)\sigma_k(m) &= \left(\frac{2^{3k}-1}{2^k-1}\right)^2.\frac{3^{2k}-1}{3^k-1}. \text{ But } \sigma_k(nm) = \frac{2^{5k}-1}{2^k-1}.\frac{3^{2k}-1}{3^k-1}. \end{aligned}$$

If $\sigma_k(n)\sigma_k(m) = \sigma_k(nm)$, then

$$\left(\frac{2^{3k}-1}{2^k-1}\right)^2 = \frac{2^{5k}-1}{2^k-1};$$

which is not true always. For example, $k = 1$ produces $49 = 31$.

(ii) For any prime power $p^\alpha, k \geq 1$

$$\sigma_k(p^\alpha) = 1 + p^k + p^{2k} + \cdots + p^{\alpha k} = \frac{p^{(\alpha+1)k}-1}{p^k-1}. \tag{2.3}$$

So, if $p_1^{r_1}p_2^{r_2}...p_s^{r_s}$ is the prime factorization of a positive integer n, then since σ_k is multiplicative we have

$$\sigma_k(n) = \prod_{j=1}^{s} \sigma_k\left(p_j^{r_j}\right) = \prod_{j=1}^{s} \frac{p_j^{(r_j+1)k} - 1}{p_j^k - 1} = \prod_{p^\alpha || n} \frac{p^{(\alpha+1)k} - 1}{p^k - 1}. \tag{2.4}$$

Furthermore, since

$$\tau\left(p_j^{r_j}\right) = (r_j + 1)$$

for each $j = 1, 2, ..., s$;

$$\tau(n) = \prod_{1 \le j \le s} (r_j + 1);$$

for $n = p_1^{r_1}p_2^{r_2}...p_s^{r_s}$.

(b) (Euler phi function).

Let $n \in \mathbb{N}$ and define

$$\varphi(n) = |\{z \in \mathbb{N} : z \le n, \gcd(z, n) = 1\}|,$$

where for every set A, $|A|$ is the cardinality of A.

(i) For every n

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{2.5}$$

(ii) φ is multiplicative but not completely-multiplicative.

(c) (Moebius function and the Moebius Inversion formula).

Let $n \in \mathbb{N}$ and define

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } p^2 | n \text{ for some prime } p \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}. \tag{2.6}$$

In general, we call an integer n *square-free* if for every prime p, $p^2 \nmid n$. So, if n is not square-free then $\mu(n) = 0$.

(i) μ is multiplicative.

(ii)

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{otherwise} \end{cases} \tag{2.7}$$

and

(iii) (Moebius Inversion formula) if f, g are arithmetic functions and

$$f(n) = \sum_{d|n} g(d)$$

then

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right). \tag{2.8}$$

To see this, given $f(n) = \sum_{d|n} g(d)$ then it is easy to see that

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right).$$

Also,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} g(k) = \sum_{k|n} g(k) \sum_{d|\frac{n}{k}} \mu(d) = g(n).$$

In (2.8), we defined $f(n) = \sum_{d|n} g(d)$. If g is multiplicative, then f is multiplicative since for $a, b \in \mathbb{N}$, $\gcd(a, b) = 1$, we have

$$f(ab) = \sum_{d|ab} g(d) = \sum_{d_1|a} g(d_1) \sum_{d_2|b} g(d_2) = f(a) f(b).$$

In fact, g is multiplicative if and only if f is multiplicative. Furthermore, given two arithmetic functions $f, g : \mathbb{N} \longrightarrow \mathbb{C}$, we define a new arithmetic function $f * g : \mathbb{N} \longrightarrow \mathbb{C}$, called the *Dirichlet convolution* of f and g, by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right). \tag{2.9}$$

It is easy to see that if f and g are multiplicative then so is $f * g$.

(d) (Trivial multiplicative functions).

(i) (Unit function): $I(n) = 1, \forall n \in \mathbb{N}$.

(ii) (Identity function): $Id(n) = n, \forall n \in \mathbb{N}$.

(iii) $e(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{otherwise} \end{cases}$.

The functions I, Id and e are completely-multiplicative.

(e) (Von Mangoldt function).

For each positive integer n, define

$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^m \text{ for some } m \in \mathbb{N} \\ 0, & \text{otherwise} \end{cases}$.

2.1.1 Euler's summation formula and summation by parts

Let $a(n)$ be an arithmetic function and consider the sums

$$\sum_{y<n\leq x} a(n)$$

and

$$\sum_{y<n\leq x} a(n) f(n);$$

where f is a function with a continuous derivative on $[y, x]; x, y \in \mathbb{R}$.

Theorem 11 *(Euler's summation formula) Let $f : [y, x] \subset \mathbb{R}^+ \longrightarrow \mathbb{C}$ be a function with a continuous derivative on its domain. Then*

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)\,dt + \int_y^x \{t\} f'(t)\,dt - \{x\} f(x) + \{y\} f(y) \qquad (2.10)$$

where $\{t\} = t - [t]$

Theorem 12 *(Summation by parts) Let $f : [y, x] \subset \mathbb{R}^+ \longrightarrow \mathbb{C}$ be a function with continuous derivative on its domain . If $a : \mathbb{N} \longrightarrow \mathbb{C}$ is an arithmetic*

function, then

$$\sum_{y<n\leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t)\, dt \qquad (2.11)$$

where $A(t) = \sum_{n\leq t} a(n)$. *In particular, if* $y = 1$,*we have*

$$\sum_{n\leq x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t)\, dt.$$

Theorem 13 *Let* $A, B \in \mathbb{R}, A < B$ *and* $A < \alpha_1 \leq \cdots \leq \alpha_n \leq b\,(\alpha_1, ..., \alpha_n \in \mathbb{N})$, $c_1, ..., c_n \in \mathbb{C}$ *and* $f(x) = \sum_{\alpha_k \leq x} c_k, x \in \mathbb{R}$. *If* $g \in C^1([A, B])$ *then*

$$\sum_{k=1}^{n} c_k g(\alpha_k) = f(B) g(B) - \int_A^B f(x) g'(x)\, dx. \qquad (2.12)$$

Proof.

$$\begin{aligned} f(B) g(B) - \sum_{k=1}^{n} c_k g(\alpha_k) &= \sum_{k=1}^{n} c_k (g(B) - g(\alpha_k)) \\ &= \sum_{k=1}^{n} c_k \int_{\alpha_k}^{B} g'(x)\, dx \\ &= \int_{\alpha_k}^{B} \sum_{\alpha_k \leq x} c_k g'(x)\, dx \\ &= \int_{\alpha_k}^{B} f(x) g'(x)\, dx. \end{aligned}$$

▪ Using theorems 11-13, one can prove the following statements.

(i)

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \log x + O(1);$$

(ii)

$$\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1);$$

(iii)

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+A+O\left(\frac{1}{\log x}\right)$$

for some constant A

(iv)

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)=e^{-A}\left(1+O\left(\frac{1}{\log x}\right)\right)$$

for some constant A. The statement

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+A+O\left(\frac{1}{\log x}\right)$$

clearly implies that there are infinitely many prime numbers since $\log\log x$ is increasing on the interval (a,b), $a<b$ for which $\log a>1$.

2.1.2 Dirichlet series and Euler product of Dirichlet series.

Definition 2: Let f be an arithmetic function, $s\in\mathbb{C}, s=\sigma+it$, then the series

$$D_f(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s} \tag{2.13}$$

is called the *Dirichlet series* of f.

It is easy to show that $D_f(s)\,D_g(s)=D_{f*g}(s)$ for arithmetic functions f,g and $s\in\mathbb{C}$. In fact, if $D_f(s)$ and $D_g(s)$ converge absolutely at s then $D_{f*g}(s)$ converges absolutely at s. In the case where g is the convolution inverse of f and $D_f(s)$, $D_g(s)$ converge absolutely at s then we have

$$D_g(s)=\frac{1}{D_f(s)}.$$

It is important to note that the absolute convergence of $D_f(s)$ does not imply the absolute convergence of the Dirichlet series of the convolution inverse of f.

Given any Dirichlet series $D_f(s)$, the number $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$ is called an *abscissa of convergence* of the series if the series converges for all $\sigma > \sigma_c$. Usually we set $\sigma_c = -\infty$ when the series converges on the entire complex plane. On the other hand, if the series converges nowhere, we write $\sigma_c = +\infty$. Therefore every Dirichlet series $D_f(s)$ must have an abscissa of convergence $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$ and it is known that $D_f(s)$ must represent an analytic function on the half-plane $\{s : \sigma > \sigma_c\}$.

Example 3: (Dirichlet series of some arithmetic functions)

(i) The Dirichlet series for $e(n)$ is

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

(ii) The Dirichlet series for the unit function $I(n)$ is

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

$\mu * I = e$, $\sum_{n=1}^{\infty} 1/n^s$ and $\sum_{n=1}^{\infty} \mu(n)/n^s$ converge absolutely for $\sigma > 1$, therefore we have

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 \Longleftrightarrow \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} \text{ for } \sigma > 1. \tag{2.14}$$

(iii) We have

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

for $\sigma > 2$.

(iv) $d(n) = (I * I)(n)$, so

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(I * I)(n)}{n^s} = \zeta(s)^2.$$

(v)

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

for $\sigma > 1$. Since, $\Lambda * I = \log$,

$$\sum_{n=1}^{\infty} \frac{\log(n)}{n^s} = -\zeta'(s).$$

Given a multiplicative arithmetic function f, the Dirichlet series of f can be expressed as the following product

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{f\left(p^k\right)}{p^{ks}}\right) \tag{2.15}$$

where

(i) $D_f(s)$ converges absolutely at s if and only if

$$\prod_p \left(1 + \sum_{k=1}^{\infty} \frac{f(p^k)}{p^{ks}}\right)$$

converges absolutely at s.

(ii) $\prod_p \left(1 + \sum_{k=1}^{\infty} f\left(p^k\right)/p^{ks}\right)$ converges absolutely at s if and only if

$$\sum_{k=1}^{\infty} \left|\frac{f(p^k)}{p^{ks}}\right| < \infty.$$

This follows from the theory on the convergence of infinite products and we will justify this claim in the next section. The product $\prod_p \left(1 + \sum_{k=1}^{\infty} f\left(p^k\right)/p^{ks}\right)$ is called the *Euler-product* of the Dirichlet series $D_f(s)$. In the case that f is completely-multiplicative, we have

$$\prod_p \left(1 + \sum_{k=1}^{\infty} \frac{f\left(p^k\right)}{p^{ks}}\right) = \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{f(p)^k}{p^{ks}}\right) = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}. \tag{2.16}$$

Example 4: (Euler-product of some Dirichlet series)

(i) The function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ has Euler-product

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

$\sigma > 1$.

(ii) $1/\zeta(s)$ has Euler-product

$$\prod_p \left(1 - \frac{1}{p^s}\right), \sigma > 1.$$

(iii) If f is completely-multiplicative and has a convolution inverse g with Dirichlet series $D_g(s)$, then $D_g(s)$ has Euler-product

$$\prod_p \left(1 - \frac{f(p)}{p^s}\right)$$

which is valid wherever $D_g(s)$ and $D_f(s)$ converge absolutely.

An important Dirichlet series used in Number Theory is that associated with the unit function. The Riemann Zeta function, defined for $s \in \mathbb{C}, s = \sigma + it$ is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2.17}$$

Riemann studied $\zeta(s)$ as a complex function and this gave him deep insight into the distribution of prime numbers. For example he was able to show that $\zeta(s)$ satisfies the functional equation

$$\pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s) = \pi^{-\frac{1}{2}(1-s)}\Gamma\left(\frac{1}{2}(1-s)\right)\zeta(1-s). \tag{2.18}$$

From the functional equation he was able to deduce that the only zeros of the zeta function satisfying $\sigma < 0$ are the negative even integers. These zeros are usually referred to as the *trivial zeros* of $\zeta(s)$. The *non-trivial zeros,* he conjectured, lie on the line $\sigma = 1/2$ in the so-called *critical strip* $0 \leq \sigma \leq 1$.

2.2 On convergence of infinite product of complex numbers

Let $\alpha_1, ..., \alpha_n \in \mathbb{C}, n \in \mathbb{N}$, $\lambda_n = \prod_{k=1}^{n}(1 + \alpha_k)$, $\lambda_n^* = \prod_{k=1}^{n}(1 + |\alpha_k|)$ and $\lambda = \prod_{k=1}^{\infty}(1 + \alpha_k)$ if the limit $\lim_{n\to\infty} \lambda_n$ exists. Then we have the following

statements which can be used to derive results concerning Euler products of Dirichlet's series:

Theorem 14 *(i) If* $\alpha_1, ..., \alpha_n \in \mathbb{C}, n \in \mathbb{N}$, *then*
(a) $\lambda_n^* \leq e^{|\alpha_1|+...+|\alpha_n|}$ *and*
(b) $|\lambda_n - 1| \leq \lambda_n^* - 1$.
(ii) λ *converges whenever the sum* $\sum_{n=1}^{\infty} |\alpha_n|$ *converges and* $\lambda = 0$ *if and only if* $\alpha_n = -1$ *for some* $n \in \mathbb{N}$.
(iii) Given any bijection $f : \mathbb{N} \longrightarrow \mathbb{N}$, *we have*

$$\lambda = \prod_{k=1}^{\infty} \left(1 + \alpha_{f(k)}\right).$$

In theorem 14, we can replace the sequence of complex numbers with a sequence of bounded functions on a set $B \subseteq \mathbb{C}$.

Theorem 15 *(i) If* $h_1, ..., h_n, n \in \mathbb{N}$ *is a sequence of bounded functions on* $B \subseteq \mathbb{C}$ *such that* $\sum_{n=1}^{\infty} |h_n(s)|$ *converges uniformly on* B, *then*

$$f(s) = \prod_{k=1}^{\infty} (1 + h_k(s))$$

converges uniformly on B *and* $f(x) = 0$ *for some* $x \in B$ *if and only if* $h_k(s) = -1$ *for some* $k \in \mathbb{N}$.
(ii) Given any bijection $f : \mathbb{N} \longrightarrow \mathbb{N}$, *we have*

$$f(s) = \prod_{k=1}^{\infty} \left(1 + h_{f(k)}(s)\right).$$

Theorem 16 *Suppose* $\alpha_n, n \in \mathbb{N}$ *are complex numbers then* $\prod_{k=1}^{\infty} (1 + \alpha_k)$ *converges if and only if* $\sum_{k=1}^{\infty} \alpha_k < \infty$.

Proof. $\sum_{k=1}^{\infty} \alpha_k < \infty \Longrightarrow \sum_{n=1}^{\infty} |\alpha_n|$ converges and so $\prod_{k=1}^{\infty} (1 + \alpha_k)$ converges. Conversely, $\prod_{k=1}^{\infty} (1 + \alpha_k)$ converges means that for every $m \in \mathbb{N}$,

$$\prod_{k=1}^{m} (1 + \alpha_k) \leq \prod_{k=1}^{\infty} (1 + \alpha_k) < \infty.$$

But $\sum_{k=1}^{m} \alpha_k \leq \prod_{k=1}^{m} (1 + \alpha_k)$ for every m and so $\sum_{k=1}^{\infty} \alpha_k$ converges. ∎

2.3 Primes in Arithmetic progressions

We know there are infinitely-many primes but a lot is still not known about what type of polynomials admit infinitely-many primes. For example, it is obvious that if the polynomial

$$f(x) = \sum_{r=0}^{k} a_r x^r, (a_0, a_1, ..., a_k \in \mathbb{Z}); f : \mathbb{Z} \longrightarrow \mathbb{Z}$$

admits infinitely-many primes then we should have $\gcd(a_0, a_1, ..., a_k) = 1$. Is this condition sufficient? For $k = 1$, Dirichlet gave a positive result and this section is dedicated to some of the basic ideas behind Dirichlet's famous theorem, stated below.

Theorem 17 *(Dirichlet) If $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$ then there are infinitely many primes p satisfying the condition $p \equiv b \pmod{a}$.*

2.3.1 Sketch of Dirichlets proof

First, we give a sketch of Euler's proof concerning the infinitude of primes, using properties of the Riemann Zeta function ζ.

To prove there are infinitely many primes, we can restrict ourselves to $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s, \mathrm{Re}(s) > 1$. We have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}, \mathrm{Re}(s) > 1. \tag{2.19}$$

Suppose there are finitely-many primes $p_1, p_2, ..., p_k$, then we should have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^s}\right)^{-1}, \mathrm{Re}(s) > 1.$$

$$\lim_{s \longrightarrow 1^+} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^s}\right)^{-1} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)^{-1} < \infty \text{ and } \lim_{s \longrightarrow 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ diverges.} \tag{2.20}$$

From (2.20), we have a contradiction. There must be infinitely-many primes. It is also possible to show that the series $\sum_p 1/p$ diverges. First, we note that

$$\zeta(s) = \frac{1}{s-1} + O(1). \tag{2.21}$$

This follows from the observation that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \geq \int_1^{\infty} \frac{dx}{x^s} = \frac{1}{s-1} \text{ and } \sum_{n=1}^{\infty} \frac{1}{n^s} \leq 1 + \int_1^{\infty} \frac{dx}{x^s} = 1 + \frac{1}{s-1}.$$

So,

$$\frac{1}{s-1} \leq \zeta(s) \leq \frac{s}{s-1} = 1 + \frac{1}{s-1} \tag{2.22}$$

and the result follows. Taking logs(at least one natural log exists and is well-defined for $\mathrm{Re}(s) > 1$) of both sides of (2.19), we have

$$\begin{aligned}
\log \zeta(s) &= \log \left(\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \right), \mathrm{Re}(s) > 1 \\
&= \sum_p \log \left(1 - \frac{1}{p^s}\right)^{-1}, \mathrm{Re}(s) > 1 \\
&= \sum_p \left(\frac{1}{p^s} + O\left(\frac{1}{p^s}\right) \right), \mathrm{Re}(s) > 1, \text{since} \left| \frac{1}{\mathrm{p^s}} \right| \leq 1/2.
\end{aligned}$$

Now,

$$\sum_p \left(\frac{1}{p^s} + O\left(\frac{1}{p^s}\right) \right) = \sum_p \frac{1}{p^s} + O\left(\sum_p \frac{1}{p^s} \right) = \sum_p \frac{1}{p^s} + O(1),$$

$\mathrm{Re}(s) > 1$ since $\sum_p 1/p^s < \infty$ for $\mathrm{Re}(s) > 1$. Therefore,

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + O(1), \mathrm{Re}(s) > 1. \tag{2.23}$$

So $\log\left(1/(s-1) + O(1)\right) = \sum_p 1/p^s + O(1), \mathrm{Re}(s) > 1$. This means that

$$\sum_p \frac{1}{p^s} = \log\left(\frac{1}{s-1}\right) + O(1), \mathrm{Re}(s) > 1 \tag{2.24}$$

and the result follows from (2.24) by letting $s \longrightarrow 1$ from the right. In order to create an equation similar to the one in (2.24) for the sum

$$\sum_{p \equiv b (\text{mod } a)} \frac{1}{p^s},$$

we need to replace the completely multiplicative function
$I : \mathbb{N} \longrightarrow \mathbb{Z}, (I(x) = 1, \forall x \in \mathbb{N})$, in (2.19), with a general completely multiplicative function that will allow us to extract specific primes in the sequence $an + b, a, b \in \mathbb{Z}, \gcd(a, b) = 1$. Dirichlet constructed just the right kind of function.

2.3.2 Note on Dirichlet Characters

Definition 3: Let $a \in \mathbb{N}$. A function $\chi : \mathbb{N} \longrightarrow \mathbb{C}$ is called a *Dirichlet character*$(\text{mod } a)$, written $\chi (\text{mod } a)$, if it satisfies the following conditions.
(i) there exists at least one $n \in \mathbb{N}$ such that $\chi(n) \neq 0$;
(ii) for every $n, m \in \mathbb{N}, \chi(nm) = \chi(n)\chi(m)$;
(iii) for every $n \in \mathbb{N}, \chi(n + a) = \chi(n)$ and
(iv) $\chi(n) = 0$, if $\gcd(a, n) > 1$.

Since $\chi (\text{mod } a)$ is a multiplicative arithmetic function for every $a \in \mathbb{N}$, $\chi(n) \neq 0$ for some $n \in \mathbb{N}$ implies that $\chi(1) = 1$. Also, if $n \in \mathbb{N}$ and $\gcd(a, n) = 1$ then $n^{\phi(a)} \equiv 1 (\text{mod } a)$ and this implies that
$\chi(n)^{\phi(a)} = 1$ (i.e. $\chi(n)$ is a $\phi(a) - th$ root of unity). Therefore, there are at most $\phi(a)$ distinct characters$(\text{mod } a)$. The obvious one(called the *principal character*) is defined as follows

$$\chi_0(n) = \begin{cases} 1, & \gcd(a, n) = 1 \\ 0, & \gcd(a, n) > 1 \end{cases}. \tag{2.25}$$

Since $\chi (\text{mod } a)$ is a complex-valued arithmetic function, it is easy to check that for any $n \in \mathbb{N}, \overline{\chi(n)} = \overline{\chi}(n)$, where $\overline{\chi} = \chi^{-1}$, and that the product of two characters $(\text{mod } a)$ is another character$(\text{mod } a)$.

Theorem 18 *(1) Let $a \in \mathbb{N}$ and $\chi \pmod{a}$ a Dirichlet character. Then (i)*

$$\sum_{n \pmod{a}} \chi(n) = \begin{cases} \phi(a), & \chi = \chi_0 \\ 0, & \text{otherwise} \end{cases}. \tag{2.26}$$

(ii) If χ and ψ are two characters $\pmod{a}$ then

$$\sum_{n \pmod{a}} \chi(n)\overline{\psi}(n) = \begin{cases} \phi(a), & \chi = \psi \\ 0, & \text{otherwise} \end{cases}. \tag{2.27}$$

(2) If $g \pmod{a}$ is given and $\Delta(a)$ is the set of all characters $\pmod{a}$ then

$$\sum_{\chi \in \Delta(a)} \chi(n)\overline{\chi}(g) = \begin{cases} \phi(a), & n \equiv g \pmod{a} \\ 0, & \text{otherwise} \end{cases}. \tag{2.28}$$

Let χ_1 and χ_2 be characters and a_1, a_2 positive integers satisfying $a_1 | a_2$. Given $\chi_2 \pmod{a_2}$ and $\chi_1 \pmod{a_1}$, we say χ_1 *induces* χ_2 if for all integers n we have

$$\chi_2(n) = \begin{cases} \chi_1(n), & \text{if } \gcd(n, a_2) = 1 \\ 0, & \text{otherwise} \end{cases}. \tag{2.29}$$

The smallest possible positive integer t such that there exists a character $\chi \pmod{t_2}$ which induces χ_2 is called the *conductor* of χ_2. If $t = a_2$, we say χ_2 is a primitive character. Furthermore, given a character $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, we define its Fourier transform by

$$\hat{\chi}(n) = \sum_{x=1}^{q} \chi(x) e^{(-xn/q)} \tag{2.30}$$

where $e(x) = e^{2\pi i x}, x \in \mathbb{R}$. The Gauss Sum of χ is defined by

$$\tau(\chi) = \sum_{x=1}^{q} \chi(x) e(x/q) \tag{2.31}$$

and one can deduce the relation $\overline{\hat{\chi}(n)} = \tau(\overline{\chi})\chi(n)$, whenever $\gcd(n, q) = 1$.

Note, that from (2.28), we get

$$\frac{1}{\phi(a)} \sum_{\chi \in \Delta(a)} \chi(n)\overline{\chi}(g) = \begin{cases} 1, & n \equiv g \pmod{a} \\ 0, & \text{otherwise} \end{cases}. \tag{2.32}$$

We can use (2.32) to extract primes that belong to the residue class $g \,(\text{mod } a)$. Define, for the character $\chi \,(\text{mod } a)$, the function

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \text{Re (s)} > 1, \text{ since } (|\chi(\text{p})| \leq 1). \tag{2.33}$$

We have

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + O(1), \text{Re (s)} > 1. \tag{2.34}$$

Given $g \,(\text{mod } a)$, we can then use (2.32) to form

$$\begin{aligned} \sum_{p \equiv g (\text{mod } a)} \frac{1}{p^s} &= \frac{1}{\phi(a)} \sum_{\chi \in \Delta(a)} \overline{\chi}(g) \sum_p \frac{\chi(p)}{p^s}, \text{Re (s)} > 1 \\ &= \frac{1}{\phi(a)} \sum_{\chi \in \Delta(a)} \overline{\chi}(g) \log L(s,\chi) + O(1), \text{Re (s)} > 1. \end{aligned}$$

Now,

$$\frac{1}{\phi(a)} \sum_{\chi \in \Delta(a)} \overline{\chi}(g) \log L(s,\chi) + O(1) = \frac{1}{\phi(a)} \log\left(\frac{1}{s-1}\right) + O(1).$$

The equality above holds because for $\chi \neq \chi_0, L(s,\chi)$ is not zero or negative infinity. That is, $\log L(s,\chi)$ is bounded as $s \longrightarrow 1^+$. This was the heart of Dirichlet's proof.

2.4 General setup of elementary sieve theory

The general setup of sieve theory can be summarized as follows.

Let A be a set of positive integers. We present some basic definitions and a fundamental result from sieve theory.

(i) $A_d = \{a \in A : a \equiv 0 \,(\text{mod } d)\}, d \in \mathbb{N}$,

(ii) $A(z) = \{a \in A : a \leq z\}, A_d(z) = \{a \in A : a \leq z, d|a\}, z \in \mathbb{N}$,

(iii) $\mathbf{P}$, the set of primes,

(iv) $\mathbf{P}(z) = \prod_{p \in \mathbf{P}, p \leq z} p$,

(v) $|B|$, the cardinality of $B \subset \mathbb{N}$,
(vi) $S(A;\mathbf{P}(z),x) = \{y \in A(z) : \gcd(y,\mathbf{P}(z)) = 1, y \leq x\}, x \in \mathbb{N}$, the object whose size we want to estimate,
(vii) if $|A| < \infty$, and $p \in \mathbf{P}$, then we define $\omega(p)$ such that $(\omega(p)/p)x$ is a good estimate to $A_p(x)$. If d is square-free then we have $\omega(d) = \prod_{p|d} p$. Also, set

$$R_d(x) = |A_d(x)| - \frac{\omega(d)}{d}x \text{ and } T(z) = \prod_{p|\mathbf{P}(z)}\left(1 - \frac{\omega(p)}{p}\right). \tag{2.35}$$

$T(z)$ is close to the probability that an element $y \in A(z)$ is co-prime to $\mathbf{P}(z)$. So, we should have

$$S(A;\mathbf{P}(z),x) = x\prod_{p|\mathbf{P}(z)}\left(1 - \frac{\omega(p)}{p}\right) + R(x,z) \tag{2.36}$$

where $R(x,z)$ is the remainder term. The general objective of sieve theory is to estimate the size of the set $S(A;\mathbf{P}(z),x)$.

Notice that

$$\begin{aligned}
S(A;\mathbf{P}(z),x) &= \sum_{n\in A, n\leq x}\sum_{d|\gcd(n,\mathbf{P}(z))}\mu(d)\\
&= \sum_{d|\mathbf{P}(z)}\mu(d)|A_d(x)|\\
&= \sum_{d|\mathbf{P}(z)}\mu(d)\left(\frac{\omega(d)}{d}x + R_d(x)\right)\\
&= x\prod_{p|\mathbf{P}(z)}\left(1 - \frac{\omega(p)}{p}\right) + \sum_{d|\mathbf{P}(z)}\mu(d)R_d(x)\\
&= x\prod_{p|\mathbf{P}(z)}\left(1 - \frac{\omega(p)}{p}\right) + l\sum_{d|\mathbf{P}(z)}R_d(x), \text{for some } |l| \leq 1.
\end{aligned}$$

Suppose $|R_d(x)| \leq \omega(d)$ and $\omega(p) \leq g$ for some constant g. Then

$\sum_{d|\mathbf{P}(z)} R_d(x) \leq \prod_{p|\mathbf{P}(z)} (1+g) = (1+g)^{\pi(z)}$, where $\pi(z)$ is the number of primes less than or equal to z. Note that the term $(1+g)^{\pi(z)}$, is exponential and so the estimate is not very good. There are methods in sieve theory that focus on reducing this error term. The following statement is therefore a crude result.

Theorem 19 *Let x be sufficiently large and $z < x$, then there exists $l\,(= l(z), |l| \leq 1)$, such that*

$$S(A; \mathbf{P}(z), x) = x \prod_{p|\mathbf{P}(z)} \left(1 - \frac{\omega(p)}{p}\right) + l \sum_{d|\mathbf{P}(z)} R_d(x).$$

In addition, if we have $|R_d(x)| \leq \omega(d)$ and $\omega(p) \leq g$ for some constant g then

$$S(A; \mathbf{P}(z), x) = x \prod_{p|\mathbf{P}(z)} \left(1 - \frac{\omega(p)}{p}\right) + O\left((1+g)^{\pi(z)}\right).$$

If we are interested in sieving out a large number of residue classes modulo each prime then the Large sieve is an appropriate tool to use. The reader is referred to [36,39] for notes on the Large sieve. We state the theorem of the Large sieve in two forms below.

Theorem 20 *(Large Sieve - arithmetic version) Let $T \subset \{M+1, M+2, ..., M+N\}$ and $\{G_p : p < z\}$ be a collection of sets such that $G_p \subset \mathbb{Z}/p\mathbb{Z}$ for each $p < z$. Then*

$$|\{n \in T : n \notin G_p \pmod{p}, \forall p < z\}| \leq \left(\pi N + z^2\right) / \left(\sum_{m<z} \mu^2(m) h(m)\right) \tag{2.37}$$

where

$$h(m) = \prod_{p|m} \left(\frac{|G_p|/p}{1 - |G_p|/p}\right) = \prod_{p|m} \frac{|G_p|}{p - |G_p|}.$$

Theorem 21 *(Large Sieve - trigonometric version) Let* $\{a_n\}_{n=1}^{N}$ *be a sequence of complex numbers. Consider a set of* $\delta-$ *space real numbers* $(|\alpha_i - \alpha_j| \geq \delta, \forall i \neq j)$ $\{\alpha_1, ..., \alpha_R\}$. *Then*

$$\sum_{r=1}^{R} \left| \sum_{n=1}^{N} a_n e(n\alpha_r) \right| \leq (\pi N + 1/\delta) \sum_{n=1}^{N} |a_n|^2 . \tag{2.38}$$

Selberg[46] showed that the above theorem holds with $N + 1/\delta - 1$ instead of $\pi N + 1/\delta$.

The following two theorems are important statements obtained using sieve methods. Both are related to primes in arithmetic progressions. Define

$$\pi(x; q, a) = |\{p : p \equiv a \pmod{q}, p \leq x\}| \tag{2.39}$$

then one should expect

$$\lim_{x \longrightarrow \infty} \frac{\pi(x; q, a)}{Li(x)} = \frac{1}{\phi(a)}, \tag{2.40}$$

where $Li(x) \sim \pi(x)$. In fact, Bombieri and Vinogradov showed (independently) the following statement.

Theorem 22 *(Bombieri-Vinogradov [6])Let* $A > 0$. *There exists a constant* $S(A)$ *such that*

$$\sum_{q \leq x^{1/2}/(\log x)^S} E(x; q) \ll_A \frac{x}{(\log x)^A} \ (x \geq 2) \tag{2.41}$$

where

$$E(x; q) = \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y; q, a) - \frac{li(y)}{\phi(q)} \right| . \tag{2.42}$$

Another important result related to $\pi(x; q, a)$ is the Brun-Titchmarsch inequality.

Theorem 23 *(Brun-Titchmarsch (Kelvin Ford) [8])For* $1 \leq q < x, (a, q) = 1$, *we have*

$$\pi(x; q, a) \leq \frac{2x}{\phi(q) \log(x/a)}. \tag{2.43}$$

2.5 Primes in short-intervals

2.5.1 Prime counting function

Let $x \in \mathbb{R}$, the prime counting function defined as $\pi(x) = \sum_{p \leq x} 1$ was conjectured, in 1798 by Legendre, to satisfy

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1. \tag{2.44}$$

Equivalently, the statement in (2.44) can be written in the form

$$\pi(x) \sim \frac{x}{logx}$$

which is the Prime Number Theorem(PNT) without an error term. Now if we consider the function

$$Li(x) = \int_2^x \frac{dt}{\log t}, \tag{2.45}$$

studied by Gauss, it is easy to show that for a fixed $k \in \mathbb{N}$

$$Li(x) = \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \cdots + \frac{k!x}{(\log x)^{k+1}} + O\left(\frac{x}{(\log x)^{k+2}}\right), \text{ as } x \longrightarrow \infty. \tag{2.46}$$

From the statement in (2.46), we have the following result from which one can deduce the statement $Li(x) \sim \pi(x)$:

Theorem 24 *For $x \geq 2$,*

$$Li(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right), \text{ as } x \longrightarrow \infty. \tag{2.47}$$

If we introduce the Chebyschev's functions

$$\vartheta(x) = \sum_{p \leq x} \log p \text{ and } \psi(x) = \sum_{p^m \leq x} \log p \text{ for } x > 0, \tag{2.48}$$

then we have $\psi(x) = \sum_{p \leq x} [\log x/\log p] \log p$. It is a well known fact that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1, \lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1 \text{ and } \lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \tag{2.49}$$

establishing relations among the functions π, ϑ and ψ. In the 19th Century, Chebyshev proved that there exist absolute constants $0 < \lambda < \mu$ such that for sufficiently large values of $x, \lambda x/\log x \leq \pi(x) \leq \mu x/\log x$. Estimates of this form are known as Chebyshev's estimates. We give three of such estimates; (Rosser J. Barkley, Schoenfeld Lowell[44]), Chebyshev [10] and Dusart [16] respectively.

Theorem 25 *For every $x \geq 17$, $x/\log x < \pi(x)$ and for every $x > 1, \pi(x) < 1.25506x/\log x$.*

Theorem 25 can be stated in the form: for every $x \geq 17, x/\log x \leq \pi(x) \leq 1.25506x/\log x$ and this form will be useful in our proof of Dirichlet's theorem,in chapter 3.

Theorem 26 *For every $x \geq x_o$, and x_o sufficiently large; $c_1 x/\log x < \pi(x) < c_2 x/\log x$ where $c_1 \approx 0.921292$ and $c_2 \approx 1.10555043$.*

Theorem 27 *For real x, we have*

$$\pi(x) \geq \frac{x}{\log x}\left(1 + \frac{1}{\log x} + \frac{1.8}{\log^2 x}\right), x \geq 32299 \tag{2.50}$$

$$\pi(x) \leq \frac{x}{\log x}\left(1 + \frac{1}{\log x} + \frac{2.51}{\log^2 x}\right), x \geq 355991. \tag{2.51}$$

Joseph Bertrand(1822-1900) conjectured that for $n > 3$, there exists a prime p with $n < p < 2n - 1$. Chebyshev proved this conjecture, now called Bertrand's postulate, in 1850. In 2006 and 2011(respectively), Bachraoui [5] and Loo Andy [37] extended this statement by proving the following results:

Theorem 28 *(M. El Bachraoui) For every $n \geq 1$, there exists a prime p satisfying $2n \leq p \leq 3n$.*

Theorem 29 *(Loo Andy) For every $n \geq 1$, there exists a prime p satisfying $3n \leq p \leq 4n$.*

Chapter 3

Main results (Prime numbers)

In this chapter, we give alternative proofs of theorems 28 and 29 and Dirichlet's theorem. We begin with a sketch of M. El Bachraoui's proof concerning primes in the interval $[2n, 3n]$. The following inequalities hold:

(a) (i) If n is even then

$$\binom{3n/2}{n} < \sqrt{6.75}^n. \tag{3.1}$$

(ii) If n is even such that $n > 152$ then

$$\binom{3n/2}{n} > \sqrt{6.5}^n. \tag{3.2}$$

(iii) If n is odd such that $n > 7$ then

$$\binom{(3n+1)/2}{n} > \sqrt{6.75}^{n-1}. \tag{3.3}$$

(iv) If $n > 945$ then

$$\left(\frac{6.5}{\sqrt{27}}\right)^n > (3n)^{\frac{\sqrt{3n}}{2}} \tag{3.4}$$

He proved the inequalities in (3.1),(3.2),(3.3) and (3.4) using induction on n. Next, he also established the following statements:

(b) (i) If n is even then

$$\prod_{n/2<p\leq 3n/4} p \cdot \prod_{n<p\leq 3n/2} p < \binom{3n/2}{n}. \tag{3.5}$$

(i) If n is odd then

$$\prod_{(n+1)/2<p\leq 3n/4} p \prod_{n<p\leq(3n+1)/4} p < \binom{(3n+1)/2}{n}. \tag{3.6}$$

In order to show that there exists a prime p in $[2n, 3n], n \in \mathbb{N}$; M. El Bachraoui considered the number

$$\binom{3n}{2n} = \frac{(2n+1)(2n+2)...3n}{1.2.3...n} \tag{3.7}$$

for $n > 945$, since the statement is known to be true for $n \leq 945$. Clearly, if there exists a prime $p \in [2n, 3n]$, then it divides $\binom{3n}{2n}$. Hence, he considered the identity $\binom{3n}{2n} = T_1T_2T_3$ where

$$T_1 = \prod_{p\leq\sqrt{3n}} p^{\beta(p)}, T_2 = \prod_{\sqrt{3n}<p\leq 2n} p^{\beta(p)}, T_3 = \prod_{2n+1\leq p\leq 3n} p; \tag{3.8}$$

$\beta(p) > 0$. The notation used in (3.8) followed the style used in [17]. Next, he showed that:
(i) if $n \in \mathbb{N}$ then $T_2 < \sqrt{27}^n$;
(ii) if n is odd then $T_1 < (3n)^{\pi(\sqrt{3n})}$ and
(iii) $(6.5)^n < T_1T_2T_3 < (3n)^{\pi(\sqrt{3n})}\sqrt{27}^n T_3$.
Therefore,

$$T_3 > \left(\frac{6.5}{\sqrt{27}}\right)^n \frac{1}{(3n)^{\pi(\sqrt{3n})}}. \tag{3.9}$$

But since $\pi(\sqrt{3n}) < \frac{\sqrt{3n}}{2}$, we have $T_3 > 1$. Hence, the product T_3 of primes between $2n$ and $3n$ is greater than 1 and so the existence of a prime in the interval $[2n, 3n]$ follows.

3.1 Bertrand-type theorems

First, define for $x > 0$ and $k > 0$

$$\pi(x, x+k) = |\{p : x \leq p \leq x+k\}|. \tag{3.10}$$

Note that for every $x > 0$ and $k > 0, \pi(x, x+k) - (\pi(x+k) - \pi(x)) \leq 1$.

Lemma 30 *For $x \geq 17$ and $k > 0$, we have*

$$\frac{x+k}{\log(x+k)} - \frac{1.256x}{\log x} < \pi(x, x+k) < \frac{1.256(x+k)}{\log(x+k)} - \frac{x}{\log x} + 2. \quad (3.11)$$

Proof. From theorem 25, if $x \geq 17$ we have

$$\frac{x}{\log x} < \pi(x) < \frac{1.25506x}{\log x}$$

and

$$\frac{x+k}{\log(x+k)} < \pi(x+k) < \frac{1.25506(x+k)}{\log(x+k)}.$$

Therefore, $x/\log x < \pi(x) < 1.256x/\log x$ and

$(x+k)/\log(x+k) < \pi(x+k) < 1.256(x+k)/\log(x+k)$. From these inequalities, we derive

$$\frac{x+k}{\log(x+k)} - \frac{1.256x}{\log x} < \pi(x+k) - \pi(x) < \frac{1.256(x+k)}{\log(x+k)} - \frac{x}{\log x}. \quad (3.12)$$

For every $x > 0, \pi(x, x+k) \geq \pi(x+k) - \pi(x)$ and so from (3.12),

$$\pi(x, x+k) > \frac{x+k}{\log(x+k)} - \frac{1.256x}{\log x} \text{ for } x \geq 17.$$

Finally, since $x, k > 0$ and $\pi(x, x+k) - (\pi(x+k) - \pi(x)) \leq 1$, we have

$$\pi(x, x+k) < \frac{1.256(x+k)}{\log(x+k)} - \frac{x}{\log x} + 2.$$

This completes the proof. ∎

With lemma 30, we can prove the statement that for $n > 2$, there exists a prime p with $n < p < 2n$.

Theorem 31 *For $n > 2, n \in \mathbb{N}$, there exists a prime p such that $n < p < 2n$.*

Proof. For $n \geq 17$, we have

$$\pi(n, 2n) > \frac{2n}{\log(2n)} - \frac{1.256n}{\log n}.$$

It is easy to check the statement for $1 < n < 17$. Furthermore, we have

$$g(x) = \frac{2x}{\log(2x)} - \frac{1.256x}{\log x} > 2, (\forall x \geq 17)$$

and so for every $n \geq 17, n \in \mathbb{N}$, there exists at least two distinct primes $p < q$ such that $n \leq p < q \leq 2n$. Finally, for $n \geq 17, n \in \mathbb{N}$, $2n$ is composite and $\pi(x, x+k) - (\pi(x+k) - \pi(x)) \leq 1$. Therefore, there exists a prime q such that $n < q < 2n$. This completes the proof. ∎

We can extend theorem 31 to the following statement.

Theorem 32 *For $n > 2, n \in \mathbb{N}$, there exist primes p_1, p_2, such that $2n < p_1 < 3n$ and $3n < p_2 < 4n$.*

Proof. We have

$$\pi(2x, 3x) > \frac{3x}{\log(3x)} - \frac{1.256(2x)}{\log 2x}, (\forall x \geq 10) \tag{3.13}$$

and

$$\pi(3x, 4x) > \frac{4x}{\log(4x)} - \frac{1.256(3x)}{\log 3x}, (\forall x \geq 6). \tag{3.14}$$

M. El. Bachraoui verified the statement "there exists a prime p_1 such that $2n < p_1 < 3n$" for $n = 2, ..., 945$. We have

$$g(x) = \frac{3x}{\log(3x)} - \frac{1.256(2x)}{\log 2x} > 2, (\forall x \geq 40)$$

and so for every $n \geq 40, n \in \mathbb{N}$, there exists at least two distinct primes $p < q$ such that $2n \leq p < q \leq 3n$. Finally, for $n \geq 40, n \in \mathbb{N}$, $2n$ and $3n$ are composite and $\pi(x, x+k) - (\pi(x+k) - \pi(x)) \leq 1$. Therefore, there exists a prime q such that $2n < q < 3n$.

Finally, Loo Andy verified the statement "there exists a prime p_2 such that $3n < p_2 < 4n$" for $2 \leq n < e^{12}$. We have

$$h(x) = \frac{4x}{\log(4x)} - \frac{1.256(3x)}{\log 3x} > 2, (\forall x \geq 212)$$

and so for every $n \geq 212, n \in \mathbb{N}$, there exists at least two distinct primes $p < q$ such that $3n \leq p < q \leq 4n$. Therefore for $n \geq 212, n \in \mathbb{N}$, $3n$ and $4n$ are composite and $\pi(x, x+k) - (\pi(x+k) - \pi(x)) \leq 1$. This completes the proof; there exists a prime q such that $3n < q < 4n$. ∎

However, the methods in theorems 31 and 32 cannot be used to show the existence of a prime p in the interval $[4n, 5n]$ because

$$g(x) = \frac{5x}{\log(5x)} - \frac{1.256(4x)}{\log 4x} < 0, (\forall x \geq 5). \tag{3.15}$$

But we can use the idea to provide an alternative proof of Dirichlet's theorem. We do this in section 3.2.

3.2 Multiples of primes in an interval

Let $A = \{p_1, p_2, ..., p_n\}$, a set of primes. Consider the following $k-$tuples.

(i) $B(k) = (1, 2, 3, 4, 5, ..., k)$,

(ii) $B(k+a) = (1+a, 2+a, 3+a, 4+a, 5+a, ..., k+a), a \in \mathbb{N}$. How many components of $B(k)$ or $B(k+a)$ are divisible by some prime in A? Generally, it is not easy to answer this problem exactly. By the Inclusion-Exclusion principle, the number of elements in $B(k) = (1, 2, 3, 4, 5, ..., k)$ divisible by some prime in A is exactly

$$\sum_{d|p_1 p_2 ... p_n, d>1} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor$$

where $\omega(d)$ is the number of distinct prime divisors of d and μ is the Moebius function. However, there is no exact answer for the case

$$B(k+a) = (1+a, 2+a, 3+a, 4+a, 5+a, ..., k+a), a \in \mathbb{N}.$$

There are many methods in sieve theory that try to solve this problem. One of the objectives of this thesis is to show that the number of components of

$B(k)$ divisible by some prime in A is an important tool that can be used to estimate the number of components of $B(k+a)$ that are divisible by some prime in A. In fact, we will show that the number of components of $B(k+a)$ that are divisible by some prime in A is bounded above by

$$\sum_{d|p_1p_2...p_n, d>1} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor + n.$$

Most importantly, this upper-bound is best possible.

Define $P(\mathbb{N}) = \{(a, a+1, a+2, ..., a+m-1) : m, a \in \mathbb{N}, \}$. Often, we are only interested in elements of $P(\mathbb{N})$ of length k, $k \in \mathbb{N}$. By the length of an element $x \in P(\mathbb{N})$, we mean the number of components of x. In this case, we will use the set

$$P_k(\mathbb{N}) = \{y \in P(\mathbb{N}) : y \text{ has length } k\}. \tag{3.16}$$

Now, given a finite set of primes, $A = \{p_1, p_2, ..., p_n\}$ [1], write

$$P_k(\mathbb{N}, A) = \{L_k(x, A) : x = (x_1, x_2, ..., x_k) \in P_k(\mathbb{N})\} \tag{3.17}$$

where

$$L_k(x, A) = \left(\gcd\left(x_1, \prod_{p_i \in A} p_i\right), ..., \gcd\left(x_k, \prod_{p_i \in A} p_i\right)\right); \tag{3.18}$$

and $L_k^*(x, A)$ is the number of components of $L_k(x, A)$ that are divisible by some prime in A. Furthermore, if

$$I_k = \left(\gcd\left(1, \prod_{p_i \in A_k} p_i\right), \gcd\left(2, \prod_{p_i \in A_k} p_i\right), ..., \gcd\left(k, \prod_{p_i \in A_k} p_i\right)\right) \tag{3.19}$$

$\in P_k(\mathbb{N}, A)$ where $A_k = \{\text{primes less than or equal to } k\}$, we have, by the inclusion-exclusion principle,

$$L_k^*(I_k, A) = \sum_{\substack{d|p_1p_2...p_n \\ d>1}} \mu(d)^{\omega(d)+1} \lfloor k/d \rfloor = \sum_{\substack{d|p_1p_2...p_n \\ d>1}} \mu(d)^{\omega(d)+1} L_k^*(I_k, \{d\}). \tag{3.20}$$

[1] The set A will always represent a finite set of primes of the form $\{p_1, ..., p_n\}$.

In this section, we will prove that, given any $x \in P_k(\mathbb{N}, A)$, we have

$$|L_k^*(x, A) - L_k^*(I_k, A)| \leq n. \tag{3.21}$$

Lemma 33 *Let $k, n \in \mathbb{N}$ and $A = \{p_1, p_2, ..., p_n\}$. If $x \in P_k(\mathbb{N}, A)$, then*

$$L_k^*(x, A) \leq L_k^*[A] = \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ odd}} \mu(d)^{\omega(d)+1} \left\lceil \frac{k}{d} \right\rceil + \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor. \tag{3.22}$$

Proof. Let $k, n \in \mathbb{N}$ and $A = \{p_1, p_2, ..., p_n\}$ and $x \in P_k(\mathbb{N}, A)$.

$$\begin{aligned} L_k^*(x, A) &= \sum_{\substack{d|p_1p_2...p_n \\ d>1}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) \\ &= \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ odd}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) + \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ even}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}). \end{aligned}$$

$\mu(d)^{\omega(d)+1} L_k^*(x, \{d\})$ is positive whenever d is odd and it is negative whenever d is even. Furthermore, the maximum and minimum values of $L_k^*(x, \{d\})$ are $\lceil k/d \rceil$ and $\lfloor k/d \rfloor$ respectively. Therefore, we have

$$L_k^*(x, A) \leq \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ odd}} \mu(d)^{\omega(d)+1} \left\lceil \frac{k}{d} \right\rceil + \sum_{\substack{d|p_1p_2...p_n \\ d>1, \omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

∎

Theorem 34 *Let $x \in P_k(\mathbb{N}, A)$; $k \in \mathbb{N}$ and $A = \{p_1, p_2, ..., p_n\}$, a finite set of primes. Then*

$$L_k^*(x, A) \leq \sum_{\substack{d|p_1p_2...p_n \\ d>1}} \mu(d)^{\omega(d)+1} L_k^*(I_k, \{d\}) + n. \tag{3.23}$$

Before we prove this theorem, we demonstrate that the upper-bound is best possible, when $x \neq I_k$. Choose $k = 3$, $A = \{5, 7\}$ and $x = (5, 6, 7) \in P_3(\mathbb{N})$ then $L_3(x, A) = (5, 1, 7) \in P_3(\mathbb{N}, A)$ and $L_3^*(I_3, \{5\}) = L_3^*(I_3, \{7\}) = 0$. Therefore

$$\sum_{d|35, d>1} \mu(d) L_3^*(I_3, \{d\}) = 0.$$

And so,

$$L_3^*(x, A) = 0 + 2 = 2 = \sum_{d|35, d>1} \mu(d)^{\omega(d)+1} L_3^*(I_3, \{d\}) + 2.$$

Proof. (Theorem 34) Let $x \in P_k(\mathbb{N}, A); k \in \mathbb{N}$, and $A = \{p_1, p_2, ..., p_n\}$. For $n = 1$, we have

$$L_k^*(x, A) \leq \left\lceil \frac{k}{p_1} \right\rceil = \left\lfloor \frac{k}{p_1} \right\rfloor + 1 = \sum_{d|p_1, d>1} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) + 1.$$

For $n = 2$, we have

$$\begin{aligned} L_k^*(x, A) &\leq \left\lceil \frac{k}{p_1} \right\rceil + \left\lceil \frac{k}{p_2} \right\rceil - \left\lfloor \frac{k}{p_1 p_2} \right\rfloor \\ &= \left\lfloor \frac{k}{p_1} \right\rfloor + \left\lfloor \frac{k}{p_2} \right\rfloor - \left\lfloor \frac{k}{p_1 p_2} \right\rfloor + 2 \\ &= \sum_{d|p_1, d>1} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) + 2. \end{aligned}$$

So, suppose $n \geq 3$. Then we have

$$\begin{aligned} L_k^*(x, A) &= \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) \\ &= \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1, \omega(d)\ odd}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) + \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1, \omega(d)\ even}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) \\ &= \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1, \omega(d)=1}} L_k^*(x, \{d\}) + \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1, \omega(d)\ odd, \omega(d)>1}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}) \\ &+ \sum_{\substack{d|p_1 p_2 ... p_n \\ d>1, \omega(d)\ even}} \mu(d)^{\omega(d)+1} L_k^*(x, \{d\}). \end{aligned}$$

Now, lemma 33 says

$$L_k^*(x,A) \leq \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)=1}} \left\lceil \frac{k}{d} \right\rceil + \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lceil \frac{k}{d} \right\rceil$$
$$+ \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

We claim that we can replace the term

$$\sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lceil \frac{k}{d} \right\rceil \text{ with } \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor$$

and have

$$L_k^*(x,A) \leq D = \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)=1}} \left\lceil \frac{k}{d} \right\rceil + \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor$$
$$+ \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

To see this, let us suppose that there is some $y \in P_k(\mathbb{N},A)$, such that $L_k^*(y,A) > D$. Without loss of generality, suppose $L_k^*(y,A) = D+1$. Since $\sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)=1}} \left\lceil \frac{k}{d} \right\rceil$ has already attained its maximum value and $\sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor$ is negative, the extra 1, in the expression $D+1$, must come from an increment in the term

$$\sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

This means that there is some $e; (e|p_1p_2...p_n, e>1, \omega(e) \text{ odd}, \omega(e)>1)$ such that

$$L_k^*(y,A) = D+1 = \sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)=1}} \left\lceil \frac{k}{d} \right\rceil + \sum_{\substack{d|p_1p_2...p_n,d\neq e \\ d>1,\omega(d)\ odd,\omega(d)>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor + \mu(e)^{\omega(e)+1} \left\lceil \frac{k}{e} \right\rceil +$$
$$\sum_{\substack{d|p_1p_2...p_n \\ d>1,\omega(d)\ even}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{k}{d} \right\rfloor.$$

We can now show that the statement, $L_k^*(y,A) = D+1$, is impossible. To see this, write $y = (y_1, y_2, ..., y_k)$ and without loss of generality suppose

that $e|y_1$ and $L_{k-1}^{*}\left(\left(y_2,...,y_k\right),A\right)=D$. This means that
$L_{k-1}^{*}\left(\left(y_2,...,y_k\right),A\right)=\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)=1}}\left\lceil\frac{k}{d}\right\rceil+\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)\ odd,\omega(d)>1}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor$
$+\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)\ even}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor.$
Notice that e is the product of at least three distinct primes and so the inclusion term $\mu\left(e\right)^{\omega(e)+1}\left\lceil\frac{k}{e}\right\rceil$ and the inclusion-exclusion principle imply that the value of

$$\left|\sum\nolimits_{d|p_1p_2...p_n,d>1,\omega(d)\ even}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor\right|$$

must increase. Furthermore, since $\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor$ is negative whenever d is even, the assumption that $L_{k-1}^{*}\left(\left(y_2,...,y_k\right),A\right)=D$ cannot be true. Therefore, we must have $L_k^{*}\left(y,A\right)\leq D$. That is, for every $x\in P_k\left(\mathbb{N},A\right)$, we have
$L_k^{*}\left(x,A\right)\leq D=\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)=1}}\left\lfloor\frac{k}{d}\right\rfloor+n+\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)\ odd,\omega(d)>1}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor$
$+\sum_{\substack{d|p_1p_2...p_n\\ d>1,\omega(d)\ even}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor=\sum_{\substack{d|p_1p_2...p_n\\ d>1}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor+n$ as required. ∎

Corollary 35 *Let $a\in\mathbb{N},k\in\mathbb{N},a_k=(a,a+1,...,a+k-1)$ and $A=\{p_1,p_2,...,p_n\}$. Then*

$$L_k^{*}\left(a_k,A\right)\leq\sum_{\substack{d|p_1p_2...p_n\\ d>1}}\mu\left(d\right)^{\omega(d)+1}\left\lfloor\frac{k}{d}\right\rfloor+n. \tag{3.24}$$

where $\omega\left(d\right)$ is the number of distinct prime divisors of d and μ is the Moebius function.

3.3 Alternative proof of Dirichlet's theorem

In this section we give an alternative proof of Dirichlet's theorem.

Lemma 36 *For every $a,b\in\mathbb{N},b\leq a,\gcd\left(a,b\right)=1$ and $k\in\mathbb{N}$, if $\sqrt{an+b}\leq k$ and $an+b$ is composite then it is divisible by some prime p satisfying $p\leq k$.*

Proof. For every positive integer u, if u is composite then u is divisible by some p satisfying $p \leq \sqrt{u}$. So, for every $a, b \in \mathbb{N}$, if $an+b$ is composite then it is divisible by some $p \leq \sqrt{an+b}$. Therefore, if $\sqrt{an+b} \leq k$ then we have $p \leq k$. ∎

For every $m \in \mathbb{N}$, let

$$E_m = \{p : p \leq m\}. \tag{3.25}$$

Consider $\sqrt{an+b} \leq m, n \in \mathbb{N} \cup \{0\}$. We have $n \leq \lfloor (m^2-b)/a \rfloor$. To show that $an+b\,(n \in \mathbb{N} \cup \{0\}, b \leq a, \gcd(a,b) = 1)$ admits infinitely-many primes, we need to show that there are infinitely-many $m \in \mathbb{N}$ such that

$$0 < L^*_{\left\lfloor \frac{m^2-b}{a} \right\rfloor + 1}\left(\left(f(0), f(1), ..., f\left(\left\lfloor \frac{m^2-b}{a} \right\rfloor\right)\right), E_m\right) < \left\lfloor \frac{m^2-b}{a} \right\rfloor + 1 \tag{3.26}$$

where $f(n) = an+b$. Note that $(f(0), f(1), ..., f(\lfloor (m^2-b)/a \rfloor))$ has $\lfloor (m^2-b)/a \rfloor + 1$ components and $L^*_{\lfloor (m^2-b)/a \rfloor + 1}((f(0), f(1), ..., f(\lfloor (m^2-b)/a \rfloor)), E_m)$ is the number of those components that are divisible by some prime in E_m and so if this number is less than $\lfloor (m^2-b)/a \rfloor + 1$ then there is a component of $(f(0), f(1), ..., f(\lfloor (m^2-b)/a \rfloor))$ that is co-prime to all the primes in E_m. We have to show that this is the case for infinitely-many values of m.

To do this, we will prove a stronger statement.

Theorem 37 *Let $m \in \mathbb{N}$ and $E_m = \{p : p \leq m\}$. If $a, b \in \mathbb{N}, b \leq a, \gcd(a,b) = 1$ and $N \geq 17$ then there are infinitely-many $m \geq N$ such that for every $x \in P_{\lfloor (m^2-b)/a \rfloor + 1}(\mathbb{N}, E_m)$ we have*

$$L^*_{\left\lfloor \frac{m^2-b}{a} \right\rfloor + 1}(x, E_m) < \left\lfloor \frac{m^2-b}{a} \right\rfloor + 1.$$

First, we prove a lemma.

Lemma 38 *Let A be a finite set of primes, $\alpha, m, a, b \in \mathbb{N}, b \leq a, \gcd(a,b) = 1$.*

$$L_\alpha((f(m+1), f(m+2), ..., f(m+\alpha)), A) \in P_\alpha(\mathbb{N}, A) \tag{3.27}$$

where $f(n) = an + b$.

Proof. Assume the hypothesis then it is easy to see that for every $y \in \mathbb{N}$, if $y|f(g)$ and $y|f(h)$ for some $g, h \in \mathbb{N}$ then $y|(g-h)$. Furthermore, for every prime p and integers n, k; $p|f(n) \Longrightarrow p|f(n+pk)$. Therefore, the sets

$$\{L_\alpha((f(m+1), f(m+2), ..., f(m+\alpha)), A) : m \in \mathbb{N}\} \tag{3.28}$$

and

$$\{L_\alpha((m+1, m+2, ..., m+\alpha), A) : m \in \mathbb{N}\} \tag{3.29}$$

are equal. ∎

We can now prove theorem 37.

Proof. (theorem 37) Assume the hypothesis and let $x \in P_{\left\lfloor \frac{m^2-b}{a} \right\rfloor + 1}(\mathbb{N}, E_m)$ then with $g = \left\lfloor \frac{m^2-b}{a} \right\rfloor + 1$

$$\begin{aligned} L_g^*(x, E_m) &\leq \sum_{\substack{d|\prod p \\ p \in E_m, d>1}} \mu(d)^{\omega(d)+1} \left\lfloor \frac{g}{d} \right\rfloor + \pi(m), \text{(theorem 34)} \\ &\leq g - \left(\frac{g}{\log g} - \frac{1.256m}{\log m} \right) + \pi(m) + 3, \text{(lemma 30)} \\ &\leq \frac{m^2-b}{a} + 4 - \frac{\frac{m^2-b}{a}+1}{\log\left(\frac{m^2-b}{a}+1\right)} + 2\left(\frac{1.256m}{\log m}\right). \end{aligned}$$

since $\sum_{d|\prod p, p \in E_m, d>1} \mu(d)^{\omega(d)+1} \left\lfloor \frac{g}{d} \right\rfloor$ is the number of integers in the interval $[1, g]$ divisible by some prime $p \in E_m$ and so it is less than or equal to

$$g - \pi(m, g) + 2 \leq g - \left(\frac{g}{\log g} - \frac{1.256m}{\log m} \right) + 3.$$

Now

$$\frac{m^2-b}{a} + 1 - L_g^*(x, E_m) \geq \frac{\frac{m^2-b}{a}+1}{\log\left(\frac{m^2-b}{a}+1\right)} - 2\left(\frac{1.256m}{\log m}\right) - 3$$

and

$$\left(\frac{m^2-b}{a}+1\right)/\left(\log\left(\frac{m^2-b}{a}+1\right)\right)-2\left(\frac{1.256m}{\log m}\right)-3\longrightarrow\infty$$

as $m\longrightarrow\infty$. Furthermore for every $m\in\mathbb{N}$ there are finitely-many $n\in\mathbb{N}$ such that $\sqrt{an+b}\leq m$. This completes the proof. ▪

Corollary 39 *If $a,b\in\mathbb{N},b\leq a,\gcd(a,b)=1$ then there are infinitely-many primes of the form $an+b$.*

Proof. Write $f(n)=an+b$ then from (3.26) it is enough to show that there are infinitely-many $m\in\mathbb{N}$ such that

$$0<L^*_{\left\lfloor\frac{m^2-b}{a}\right\rfloor+1}\left(\left(f(0),f(1),...,f\left(\left\lfloor\frac{m^2-b}{a}\right\rfloor\right)\right),E_m\right)<\left\lfloor\frac{m^2-b}{a}\right\rfloor+1. \tag{3.30}$$

From lemma 38

$$L^*_{\left\lfloor\frac{m^2-b}{a}\right\rfloor+1}\left(\left(f(0),f(1),...,f\left(\left\lfloor\frac{m^2-b}{a}\right\rfloor\right)\right),E_m\right)\in P_{\left\lfloor\frac{m^2-b}{a}\right\rfloor+1}(\mathbb{N},E_m)$$

and applying theorem 37, the result follows. ▪

But the method above cannot be used to determine whether or not there are infinitely-many primes of the form $f(n)=n^2+1$. This is because there exists a positive integer k such that for every $n,m\in\mathbb{N}$, we have

$$L_k((f(n+1),f(n+2),...,f(n+k)),\mathbb{N})\notin P_k(\mathbb{N},E_m). \tag{3.31}$$

For example, $5|f(2)$ and $5|f(3)$ but $5\nmid 2-3$. Therefore, we cannot apply lemma 38 directly. As mentioned earlier, it is not known if there are infinitely many primes of the form n^2+1. However, since each prime p satisfying $p\equiv 1\pmod 4$ is the sum of two squares, one should expect that x^2+y^2 admits infinitely many primes. For a polynomial in two variables with degree greater than 1, the following result is well-known.

Theorem 40 *(Friedlander - Iwaniec [20]) If Λ denotes the von Mangoldt function then*

$$\sum_{\substack{a>0\\ a^2+b^4\leq x}}\sum_{b>0}\Lambda(a^2+b^4)=4\pi^{-1}\kappa x^{3/4}\left\{1+O\left(\frac{\log\log(x)}{\log(x)}\right)\right\} \tag{3.32}$$

as $x\to\infty$, where

$$\kappa=\int_0^1(1-t^4)^{1/2}dt. \tag{3.33}$$

Equivalently, this statement shows that there are infinitely-many primes of the form x^2+y^4. In a related development Heath-Brown[27] showed that x^3+2y^3 also admits infinitely-many primes.

Theorem 41 *(Heath-Brown [27], page 84) There is a positive constant c such that if $g=g(x)=(\log(x))^{-c}$ then*

$$\sum_{\substack{x<a\leq x(1+g)\\ x<b\leq x(1+g)\\ p=a^3+2b^3}}1=\sigma_0\frac{g^2x^2}{3\log(x)}1+O\left((\log\log(x))^{-1/6}\right) \tag{3.34}$$

as $x\to\infty$, where

$$\sigma_0=\prod_p\left(1-\frac{w(p)-1}{p}\right) \tag{3.35}$$

and $w(p)$ denotes the number of solutions of the congruence $x^3\equiv 2\,(\text{mod p})$.

In the next section we investigate some properties of $\lambda-$ stationary polynomials in $\mathbb{Z}[x]$.

3.4 On $\lambda-$ stationary polynomials in $\mathbb{Z}[x]$

3.4.1 Definitions and basic results

Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients and

$$\mathbb{Z}_k[x]=\{f(x)\in\mathbb{Z}[x]:\deg(f)=k\},k\geq 0. \tag{3.36}$$

For each $\lambda > 0, z \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$; consider the sequence $T_f^{\lambda}(z) = \left(a_f^{\lambda}(z,n)\right)_{n\geq 0}$ defined by

$$a_f^{\lambda}(z,n) = \begin{cases} |z|, & \text{if } n = 0 \\ max \left\{ \begin{array}{l} p \text{ prime: } p | f\left(a_f^{\lambda}(z,n-1)\right) \\ \text{and } p \leq \left(\left|f\left(a_f^{\lambda}(z,n-1)\right)\right|\right)^{\lambda} \end{array} \right\}, & \text{if it exists and } n > 0 \\ 1, & \text{otherwise} \end{cases} . \tag{3.37}$$

We say the sequence $T_f^{\lambda}(z)$ is *stationary* if there exist positive integers m, u such that for every $n \geq m$, $a_f^{\lambda}(z,n) \leq u$. Furthermore, f is said to be $\lambda-$ *stationary* if for every integer z, the sequence $T_f^{\lambda}(z)$ is stationary. Note that $\forall \lambda > 0, k \in \mathbb{N}$ and $z \in \mathbb{Z}$ the sequence $T_f^{\lambda}(z)$ is stationary if f is the zero-polynomial of degree k. This is because $a_f^{\lambda}(z,n) = 1, \forall n \geq 1$. Write

$$\lambda_f^*(z) = \min\left\{g \in \mathbb{N} : \exists y \in \mathbb{N} \text{ such that } \forall n \geq y, a_f^{\lambda}(z,n) \leq g\right\} \tag{3.38}$$

$$\text{and } \lambda_f^* = \max\left\{\lambda_f^*(z) : z \in \mathbb{Z}\right\}. \tag{3.39}$$

The number λ_f^* may not exist. If f is the zero-polynomial of any degree then $\lambda_f^* = 1$. The next result gives a condition for the existence of $\lambda_f^*(z)$.

Theorem 42 *Let $k \in \mathbb{N}, f(x) \in \mathbb{Z}_k[x]$ and $z \in \mathbb{Z}$. $\lambda_f^*(z)$ exists if and only if for every $\rho > 1$,the series $\sum_{j=1}^{\infty}\left(1/a_f^{\lambda}(z,j)\right)^{\rho}$ is divergent.*

Proof. Let $k \in \mathbb{N}, f(x) \in \mathbb{Z}_k[x]$ and $z \in \mathbb{Z}$. Suppose $\lambda_f^*(z)$ exists and there exists $\rho > 1$ such that $\sum_{j=1}^{\infty}\left(1/a_f^{\lambda}(z,j)\right)^{\rho}$ is convergent. $\sum_{j=1}^{\infty}\left(1/a_f^{\lambda}(z,j)\right)^{\rho}$ convergent implies that the sequence $\left(a_f^{\lambda}(z,n)\right)_{n\geq 1}$ contains a strictly-increasing sub-sequence $\left(b(n)\right)_{n\geq 0}$. This contradicts the assumption that $T_f^{\lambda}(z)$ is stationary.

Conversely, suppose for every $\rho > 1$, the series $\sum_{j=1}^{\infty}\left(1/a_f^{\lambda}(z,j)\right)^{\rho}$ is divergent. Then there exists a positive integer g such that $g = a_f^{\lambda}(z,n)$ for infinitely-many values of n. So there must be some $\mu, \theta\,(1 < \mu < \theta)$ such that $a_f^{\lambda}(z,\mu) = g, a_f^{\lambda}(z,\theta) = g$. Set $h_z = \max\left\{a_f^{\lambda}(z,0), ..., a_f^{\lambda}(z,\theta)\right\}$ then $h_z = \lambda_f^*(z)$ and so $\lambda_f^*(z)$ exists. ∎

Note that for each $k \in \mathbb{N}$ there exists $\lambda > 0$ and $f(x) \in \mathbb{Z}_k[x]$ such that λ_f^* does not exist. For example, choose $f(x) = x^k$ and $\lambda = 1$ then for every prime p and $n \geq 0$ we have $a_f^\lambda(p, n) = p$ and so the sequence $\left(\lambda_f^*(z)\right)_{z \geq 1}$ has a strictly-increasing sub-sequence. Therefore, λ_f^* does not exist. Furthermore, it should be obvious that if λ_f^* exists then f is $\lambda-$ stationary but the converse is not true.

Theorem 43 *Let $f(x) \in \mathbb{Z}_k[x]$, $z \in \mathbb{Z}$ and $0 < \lambda < \theta$. If $T_f^\theta(z)$ is stationary then $T_f^\lambda(z)$ is stationary.*

Proof. $T_f^\theta(z)$ stationary implies that for every $\rho > 1$ the series $\sum_{j=1}^\infty \left(1/a_f^\theta(z, j)\right)^\rho$ is divergent. Now since $\lambda < \theta$ we have $a_f^\lambda(z, j) \leq a_f^\theta(z, j)$ for every $j \in \mathbb{N}$. Therefore, $\sum_{j=1}^\infty \left(1/a_f^\theta(z, j)\right)^\rho \leq \sum_{j=1}^\infty \left(1/a_f^\lambda(z, j)\right)^\rho$ and so $T_f^\lambda(z)$ is stationary. ▪

The next theorem is easy to prove but shows the importance of the number 1 in the theory of $\lambda-$ stationary polynomials in $\mathbb{Z}[x]$.

Theorem 44 *Let $\lambda > 0$. $T_f^1(z)$ is stationary if and only if $T_f^{1+\lambda}(z)$ is stationary.*

Proof. For every $n \in \mathbb{N}$ and $z \in \mathbb{Z}$ note that $a_f^1(z, n) = a_f^{1+\lambda}(z, n)$. ▪

A natural question to ask at this point is 'what is the largest value of $\lambda \in (0, 1]$ such that given $f(x) \in \mathbb{Z}_k[x]$ and $z \in \mathbb{Z}$, $T_f^\lambda(z)$ is stationary'. For each $\lambda > 0$ define the set $\mathbb{Z}^\lambda[x] = \{f(x) \in \mathbb{Z}[x] : f \text{ is } \lambda - \text{ stationary}\}$. We have already shown that any zero polynomial belongs to $\mathbb{Z}^\lambda[x], \lambda > 0$. This gives an idea that the following theorem must be true.

Theorem 45 *For each $f(x) \in \mathbb{Z}[x], \exists \lambda > 0$ such that f is $\lambda-$ stationary.*

Before we prove this theorem, we first establish the result.

Lemma 46 *For each $f(x) \in \mathbb{Z}_k[x]$ and $z \in \mathbb{Z}$,$\exists \lambda > 0$ such that the sequence $\left(a_f^\lambda(z, n)\right)_{n \geq 1}$ is bounded above.*

Proof. Let $f(x) \in \mathbb{Z}_k[x]$, choose $\lambda = 1/2k$ then for every $z \in \mathbb{Z}$ there exists $m \in \mathbb{Z}$ such that for every $n \geq m$ we have $\left(\left|f\left(a_f^{1/2k}(z,n)\right)\right|\right)^{1/2k} \leq a_f^{1/2k}(z,n)$. To see this notice that $\lim_{x\longrightarrow\infty}\left(|f(x)|\right)^{1/2k}/x = 0$. Therefore, there exists a positive integer y such that for every $x \geq y$ we have $\left(|f(x)|\right)^{1/2k} \leq x$. Furthermore, for each z let $g_z = \max\left\{a_f^{1/2k}(z,n) : n \in \mathbb{Z}\right\} < 0$ then we have that for every n, $a_f^{\lambda}(z,n) \leq g_z$. ▪

Proof. (theorem 45) Let $f(x) \in \mathbb{Z}_k[x]$ and $z \in \mathbb{Z}$, and choose $\lambda = 1/2k$ then for every $z \in \mathbb{Z}$, $\left(a_f^{\lambda}(z,n)\right)_{n\geq 1}$ is bounded above. Therefore, f is $\lambda-$stationary. ▪

Theorem 47 *Let $f(x), g(x) \in \mathbb{Z}^y[x]$ and c be a constant. (i) If $f(x), g(x) \in \mathbb{Z}^1[x]$, then $fg(x) \in \mathbb{Z}^b[x]$ for every $b > 0$. (ii) $cf(x) \in \mathbb{Z}^y[x]$.*

Proof. (i) Let $f(x), g(x) \in \mathbb{Z}^1[x]$ then for every integer z, $n \in \mathbb{N}$,

$$a_{fg}^1(z,n) \leq \max\left\{a_f^1(z,n), a_g^1(z,n)\right\}$$

and so $1_{fg}^*(z) \leq \max\left\{1_f^*(z), 1_g^*(z)\right\}$. Therefore, $1_{fg}^*(z)$ exists. Finally, $fg(x) \in \mathbb{Z}^1[x] \Longrightarrow fg(x) \in \mathbb{Z}^b[x]$ for every $b > 0$.

(ii) Let $f(x) \in \mathbb{Z}^y[x]$ and c a constant. It is enough to prove this result for $y \leq 1$. Clearly, $y_{cf}^*(z) \leq |c|\, y_f^*(z)$ since $\left(|cf(n)|\right)^y \leq |c|\left(|f(n)|\right)^y$ for every $n \in \mathbb{N}$. Therefore,

$$a_{cf}^y(z,n) \leq \max\left\{a_c^y(z,n), a_f^y(z,n)\right\} \leq |c| \max\left\{1, a_f^y(z,n)\right\} = |c|\, a_f^y(z,n)$$

and since the sequence $\left(a_f^y(z,n)\right)_{n\geq 1}$ is bounded above, we have $cf \in \mathbb{Z}^y[x]$.

▪

The statement $f(x), g(x) \in \mathbb{Z}^b[x] \Longrightarrow fg(x) \in \mathbb{Z}^b[x]$ holds if $b \geq 1$ but is generally difficult to prove if $b \in (0,1)$ and this is the question that is of interest. We conclude this section by stating the following conjecture.

Conjecture 48 *If $b > 0$ and $f(x) \in \mathbb{Z}[x]$ then $f(x) \in \mathbb{Z}^b[x]$.*

Chapter 4

Introduction(OPNs)

4.1 σ, σ_{-1} and Φ_n

In this section, we provide important properties of the functions σ, σ_{-1}(σ, the sum of divisors function) and Φ_n(the $nth-$cyclotomic polynomial). The sum of divisors function is defined by

$$\sigma\left(p_1^{r_1}p_2^{r_2}...p_k^{r_k}\right) = \sigma\left(s\right) = \sum_{x|s, x\geq 1} x = \prod_{j=1}^{k} \frac{p_j^{r_j+1}-1}{p_j-1}.$$

The abundancy function, σ_{-1}, is defined by $\sigma_{-1}\left(n\right) = \sigma\left(n\right)/n$, $n \in \mathbb{N}$ and $\sigma_{-1}\left(n\right)$ is called the *abundancy-index* of n. We can use σ_{-1} to partition the set of positive integers as follows. For each positive integer n,

(i) $\sigma_{-1}\left(n\right) < 2 \Longleftrightarrow n$ is *deficient*,

(ii) $\sigma_{-1}\left(n\right) = 2 \Longleftrightarrow n$ is *perfect*,

(iii) $\sigma_{-1}\left(n\right) > 2 \Longleftrightarrow n$ is *abundant*.

It is interesting to note that σ_{-1} is dense [35] on $(1, \infty)$. However, P.A. Weiner [53] proved that there exists a subset of rational numbers dense in $(1, \infty)$ which do not belong to the image of σ_{-1}. A remarkable result by R.F. Ryan [45] gives a sufficient condition for some numbers to be an OPN.

Theorem 49 *(R.F. Ryan) If there exists a positive integer n and an odd*

positive integer m *such that* $2m-1$ *is a prime not dividing* n *and* $\sigma_{-1}(n) = (2m-1)/m$ *then* $n(2m-1)$ *is an odd perfect number.*

Since the divisor function is multiplicative, so is the abundancy function. For a prime p, we have $\sigma_{-1}(p) = 1 + \frac{1}{p}$ and

$$\lim_{\substack{a \to \infty \\ a \in \mathbb{N}}} \sigma_{-1}(p^a) = \frac{p}{p-1}. \tag{4.1}$$

Hence, $1 + \frac{1}{p} \leq \sigma_{-1}(p^a) \leq 1 + \frac{1}{p-1}$.

$$\sigma_{-1}(p^a) = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^a} = \frac{(p^{a+1}-1)}{p^a(a-1)},$$

therefore, for $a > b, a, b \in \mathbb{N}$, we have $\sigma_{-1}(p^a) > \sigma_{-1}(p^b)$.

The abundancy function is one of the most important tools used in the study of odd perfect numbers. In recent years, another function, the $nth-$cyclotomic polynomial, is used to study OPNs.

Definition 50 .

Let $n \in \mathbb{N}$. The *nth−cyclotomic polynomial*, $\Phi_n(x)$, is the polynomial having exactly the primitive nth roots of unity as roots. For each $x \in \mathbb{N}$,

$$\Phi_n(x) = \prod_{\substack{t^n=1 \\ ord(t)=n}} (x-t) \tag{4.2}$$

where $ord(t) = \min\{y > 0, y \in \mathbb{Z} : t^y = 1\}$. So, by definition, $\deg(\Phi_n) = n$.

We provide some interesting examples of these results, especially those that are useful in the study of OPNs.

Theorem 51 *If* $\Phi_n(x)$ *is the nth−cyclotomic polynomial then the following conditions hold.*

(i) The coefficients of Φ_n *are integers.*
(ii) $x^n - 1 = \prod_{r|n} \Phi_r(x)$.
(iii) $\Phi_n(x) = \prod_{r|n} \left(x^{n/r} - 1\right)^{\mu(r)}$.
(iv) For a positive prime p *and positive integers* n and k, *we have*

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n\left(x^{pk}\right), & \text{if } p|n \\ \Phi_n\left(x^{p^k}\right)/\Phi_n\left(x^{p^{k-1}}\right), & \text{if } p \nmid n \end{cases}.$$

Note that for arithmetic functions f and g, the product form of the Dirichlet convolution of arithmetic functions implies that if $f(n) = \prod_{r|n} g(r)$ then $g(n) = \prod_{r|n} f(n/r)^{\mu(r)}$. Therefore, in theorem 51, one can easily get (iii) from (ii) with $f(n) = x^n - 1$ and $g(n) = \Phi_n(x)$. A complete proof of (iii) can also be found in Vardi I. [53]. Furthermore, if $n = p$ then from (ii) $x^p - 1 = \prod_{r|p} \Phi_r(x) = \Phi_1(x)\Phi_p(x) \Longrightarrow \Phi_p(x) = x^{p-1} + x^{p-2} + ... + 1$.

Now, we can link the functions σ and Φ_n as follows. Let $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$,as in (2.1). Since σ is multiplicative, we have $\sigma\left(p_1^{r_1} p_2^{r_2} ... p_k^{r_k}\right) = \prod_{j=1}^{k} \left(p_j^{r_j+1} - 1\right)/p_j - 1$. $\sigma\left(p^g\right) = p^g + p^{g-1} + ... + 1 = \left(p^{g+1} - 1\right)/(p-1)$ for every prime p, positive integer g. In (ii), theorem 51, let $n = g + 1, x = p$ then we have $p^{g+1} - 1 = \prod_{r|g+1} \Phi_r(p)$. Therefore,

$$\sigma\left(p^g\right) = \frac{\prod_{r|g+1} \Phi_r(p)}{p-1}. \tag{4.3}$$

Finally, letting $\Phi_1(p) = p - 1$, in (5.3) we have

$$\sigma\left(p^g\right) = \prod_{\substack{r|g+1 \\ r>1}} \Phi_r(p). \tag{4.4}$$

Therefore, if $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ is perfect then the multiplicativity of σ implies that

$$2n = \sigma(n) = \sigma\left(p_1^{r_1} p_2^{r_2} ... p_k^{r_k}\right) = \prod_{j=1}^{k} \prod_{\substack{r|r_j+1 \\ r>1}} \Phi_r(p_j). \tag{4.5}$$

This statement, (4.5), is the most important connection between σ and Φ_n. The following theorem found in [47] was obtained in the nineteenth century.

Theorem 52 *Let q be a prime, and a, d be integers. If $a \geq 2, d \geq 3$, then the following statements hold.*

(i) If $q \mid \Phi_d(a)$, then $q \mid d$ or $q \equiv 1 \pmod{d}$.
(ii) If $q \mid \Phi_d(a)$ and $q \mid d$ then $q^2 \nmid \Phi_d(a)$.
(iii) If $(a, d) \neq (2, 6)$, then the cyclotomic number $\Phi_d(a)$ has at least one prime factor q such that $q \equiv 1 \pmod{d}$.

4.2 $k-$ perfect numbers

A positive integer g is said to be *perfect* if $\sigma(g) = 2g$. In general, g is said to be a $k-$ *perfect* number if $\sigma(g) = kg$. So, a $2-$perfect number is a perfect number. We know the general form of even perfect numbers, thanks to the following statement which characterizes all even perfect numbers.

Theorem 53 *(Euler) An even integer g is perfect if and only if $g = 2^{n-1}(2^n - 1)$ for some $n \in \mathbb{N}$ and $2^n - 1$ is prime.*

If the number $2^n - 1$ is prime, then n must be prime. To see this, assume that n is a composite. Then $n = ab$ for some positive integers $a > 1$ and $b > 1$. So then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$, which is composite, contradicting the assumption that $2^n - 1$ is prime. Furthermore, the prime $2^p - 1$ is usually called a *Mersenne prime* and currently 48 Mersenne primes are known to exist. There is a 1-1 correspondence between Mersenne primes and even perfect numbers. Therefore, if there are infinitely-many Mersenne primes then there are infinitely-many even perfect numbers.

The reader is referred to ([12],[13],[14],[52]) for different proofs of theorem 53. What about odd perfect numbers, do we have the general form of

an OPN? According to Euler, every odd perfect number must satisfy the following statement:

Theorem 54 *(Euler) If g is an odd perfect number then $g = p^k n^2$ for some prime number p and integer k satisfying $p \equiv k \equiv 1 (\text{mod } 4)$ and $\gcd(p, n) = 1$.*

Proof. First, we show that if N is an odd perfect number with prime decomposition $N = q_1^{r_1} q_2^{r_2} ... q_k^{r_k}$ then $|\{j : 1 \leq j \leq k, r_j \text{ is odd}\}| = 1$. First, if r_j is even for every $j\,(1 \leq j \leq k)$ then $\sigma\left(q_j^{r_j}\right)$ is odd for all j. Thus, $\sigma(N) = \prod_{j=1}^{k} \sigma\left(q_j^{r_j}\right)$ is odd and we have a contradiction since $\sigma(N) = 2N$.

Now suppose for some $t, s\,(1 \leq t < s \leq k), r_t$ and r_s are odd then $\sigma\left(q_j^{r_j}\right)$ is even for all $g \in \{s, t\}$. Therefore

$$\sigma(N) = \prod_{j=1}^{k} \sigma\left(q_j^{r_j}\right) = \sigma\left(q_t^{r_t}\right)\sigma\left(q_s^{r_s}\right) \prod_{\substack{1 \leq j \leq k \\ j \in \{t,s\}}} \sigma\left(q_j^{r_j}\right) = 4h$$

for some positive integer h. This contradicts our assumption that $\sigma(N) = 2N$.

Thus $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ for some positive integers $r_1, r_2, ..., r_k$; distinct primes $p, q_1, q_2, ..., q_k$ and an odd integer α. It remains to show that $\alpha \equiv p \equiv 1 (\text{mod } 4)$.

To see this suppose that $\alpha \equiv p \equiv 3 (\text{mod } 4)$. Then $(p+1) | \sigma(p^{\alpha})$, $4 | p+1$ and $(p+1) | \sigma(N)$. This is impossible, since $4 \nmid \sigma(N)$. Also, $\sigma(p^{\alpha}) \equiv 0 (\text{mod } 4)$ which is a contradiction. Therefore, $\alpha \equiv p \equiv 1 (\text{mod } 4)$. ∎

According to theorem 54, if n is an OPN then n should be of the form

$$n = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}, p \equiv \alpha \equiv 1 (\text{mod } 4) \text{ and } \gcd\left(p^{\alpha}, q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}\right) = 1, \tag{4.6}$$

where $q_1, q_2, ..., q_k$ are distinct primes. The prime number p is called the *special prime*. There are many problems related to the existence of OPNs and we can classify and list them as follows.

4.3 Old results

In this section, we provide most of what is already known about OPNs. Our focus will be on the findings of other researchers in the field.

Are there OPNs?

As at the time of writing this thesis, no odd perfect numbers had been found. But we know the following statements are true.

(i) (Euler): If n is an OPN then n should be of the form $n = p^{\alpha}q_1^{2r_1}q_2^{2r_2}...q_k^{2r_k}, p \equiv \alpha \equiv 1(\text{mod } 4)$ and $\gcd\left(p^{\alpha}, q_1^{2r_1}q_2^{2r_2}...q_k^{2r_k}\right) = 1$, where $q_1, q_2, ..., q_k$ are distinct primes. The prime number p is called the *special prime*.

(ii) (Luca and Pomerance [38]): If n is an OPN then $rad\,(n) \leq 2n^{17/26}$, where $rad\,(n) = \prod_{p|n} p$.

(iii) If n is an OPN then

- (Kanold [32]): $n > 10^{20}$;
- (Tuckerman [51]): $n > 10^{36}$;
- (Brent and Cohen [7]): $n > 10^{160}$ and $n > 10^{300}$;
- (Ochem and Rao [42]): $n > 10^{1500}$; This is the most recent result on the size of an odd perfect number, if it exists.

(v) (Touchard [50]): If n is an OPN then $n \equiv 1\,(\text{mod } 12)$ or $n \equiv 9\,(\text{mod } 36)$.

(vi) (Ore [43]): If n is an OPN then n is a *harmonic number* (a positive integer is said to be harmonic if the harmonic mean of its positive divisors is an integer).

Number of prime divisors of OPNs

If an odd perfect number exists, it must have a minimum number of prime divisors. These are some of the known results.

(i) (Hagis [23]): If n is an OPN then it has at least 8 distinct prime divisors.

(ii) (Kishore [33]): If n is an OPN then it has at least 10 distinct prime divisors.

(iii) (Nielsen [40]): If n is an OPN then it has at least 12 distinct prime divisors.

(iv) (Norton [41]): If n is an OPN and it is not divisible by 3 or 5, then it must have at least 15 distinct prime divisors, and if it is not divisible by 7, it must have at least 27 distinct prime divisors.

(v) (Hare [26]): If n is an OPN then it has must have at least 37 prime factors. He later improved this to 75 prime factors.

(vi) (Ochem and Rao [42]): If n is an OPN then it must have at least 101 prime factors.

Size of the prime factors of OPNs.

Even though there are numerous results concerning the size of different prime factors of an OPN, we are interested in the size of the largest prime divisor. The following results are well-known.

(i) (Hagis [23]): If n is an OPN then the largest prime divisor of n is greater than 10^5.

(ii) (Jenkins [29]): If n is an OPN then the largest prime divisor of n is greater than 10^7.

(iii) (Goto and Ohno[21]): If n is an OPN then the largest prime divisor of n is greater than 10^8.

Properties of $r_1, r_2, ..., r_k$ in $n = p^\alpha q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$, OPN

If $n = p^\alpha q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN, what do we know about the constants $r_1, r_2, ..., r_k$? For example, it is not known if we can have all the r_is equal.

(i) (Steuerwald [49]): Not all of the r_is can be 1.

(ii) (Kanold [32]): The r_i cannot all be equal to 2 and $\gcd(2r_1 + 1, ..., 2r_k + 1) \notin \{9, 15, 21, 33\}$.

Chapter 5

Main results

5.1 $k-$perfect numbers

The goal of this section is to prove the theorem below and give some ideas that are useful in dealing with $k-$ perfect numbers.

Theorem 55 *Let x be a $k-$perfect number with prime decomposition $x = p_1^{r_1}p_2^{r_2}...p_t^{r_t}$. If k is prime then for every $A \in C(\Gamma_x)$ we have $T_*^x(A) = \Gamma_x$. (ii) If $T_*^x(A) \neq \Gamma_x$, then x is divisible by a $g-$perfect number for some $g \in \mathbb{N}$.*

By theorem 55, if we know that $p^f||x$ for some prime p, and x is a $k-$perfect number, k prime, then we can generate Γ_x using a series of steps, defined below. But what if $k = k_1k_2(k_1, k_2 > 1, k_1 \neq k_2)$? Generally, if k is composite, it is not known if given any A we will have $T_*^x(A) = \Gamma_x$. So, theorem 55 resolves the special case where k is prime. It is obvious that one can arrive at the same result using other means but the ideas developed are interesting. We give the meaning to the notations in the theorem and give two results before we return to prove theorem 55.

Let x be a positive integer. Define, (i)$\Gamma_x = \{p^r : p^r||x, p \text{ prime}, r \in \mathbb{N}\}$, (ii) $C(\Gamma_x) = \{A \subset \Gamma_x : A \neq \varnothing, A \neq \Gamma_x\}$ (iii) for $A, B \in C(\Gamma_x)$,

$$G(A|B)=\left\{a\in\Gamma_x:\gcd\left(a,\prod_{y\in B}y\right)=1,\gcd\left(a,\sigma\left(\prod_{x\in A}x\right)\right)>1\right\}. \quad (5.1)$$

By the definition in (5.1), $G(A|B)$ can be the empty set. For example, consider $x=105=3\times5\times7$. Let $A=\{3\}$ and $B=\{5\}$; then $A,B\in C(\Gamma_x)$ and $G(A|B)=\emptyset$. Therefore, for the rest of this section we will assume that x is a $k-$perfect number. More generally, if $A_1,A_2,...,A_n\in C(\Gamma_x)$, not necessarily distinct elements; define $G(A_n|A_{n-1},...,A_1)=$

$$\left\{a\in\Gamma_x:\gcd\left(a,\prod_{y\in A_{n-1}\cup\cdots\cup A_1}y\right)=1,\gcd\left(a,\sigma\left(\prod_{x\in A_n}x\right)\right)>1\right\}. \quad (5.2)$$

Theorem 56 *Let x be a $k-$perfect number greater than 1. If $A,B,C\in C(\Gamma_x)$, then (i) $G(A|A,A)=G(A|A)$, (ii) $G(A|B,C)=G(A|B)\cap G(A|C)=G(A|B\cup C)$ and (iii) $G(A_n|A_{n-1},...,A_1)=\bigcap_{j=1}^{n-1}G(A_n|A_j)$.*

Proof. Assume the hypothesis, then (i)

$G(A|A,A)=\left\{a\in\Gamma_x:\gcd\left(a,\prod_{y\in A\cup A}y\right)=1,\gcd\left(a,\sigma\left(\prod_{x\in A}x\right)\right)>1\right\}=$

$\left\{a\in\Gamma_x:\gcd\left(a,\prod_{y\in A}y\right)=1,\gcd\left(a,\sigma\left(\prod_{x\in A}x\right)\right)>1\right\}=G(A|A).$

(ii) $G(A|B,C)=\left\{a\in\Gamma_x:\gcd\left(a,\prod_{y\in B\cup C}y\right)=1,\gcd\left(a,\sigma\left(\prod_{x\in A}x\right)\right)>1\right\}$

$=G(A|B\cup C).$

Furthermore, $\gcd\left(a,\prod_{y\in B\cup C}y\right)=1$ if and only if $\gcd\left(a,\prod_{y\in B}y\right)=1$ and $\gcd\left(a,\prod_{y\in C}y\right)=1$; therefore $G(A|B)\cap G(A|C)=G(A|B\cup C)$.

(iii) The general case follows from induction on n. ∎

Now consider the following sequence; $T_1(x,A),T_2(x,A),...,T_n(x,A),...$ defined as follows.

$$\begin{array}{lcl} T_1(x,A) & = & A \\ T_2(x,A) & = & G(T_1(x,A)|A) \\ T_3(x,A) & = & G(T_2(x,A)|T_1(x,A)) \\ & . & \\ & . & \\ & . & \\ T_{n+1}(x,A) & = & G(T_n(x,A)|T_{n-1}(x,A),...,T_1(x,A)). \end{array} \tag{5.3}$$

For each $A \in C(\Gamma_x)$, define $G^*(x,A) = T_1(x,A) \to T_2(x,A) \to \cdots \to T_m(x,A)$, where $T_{m+1}(x,A) = \varnothing$. $G^*(x,A)$ is called a *chain in* $C(\Gamma_x)$. A is the *origin* of the chain and it is easy to see that every element in $C(\Gamma_x)$ is the origin of a unique chain in $C(\Gamma_x)$. Also, for each $i\,(1 \leq i \leq m)$, $T_i(x,A)$ is called a *node in the chain.* If L is a node in a chain G, we write $L \in G$.

We also introduce a sequence of chains, $L^x(A) = (G_n^*(x,A))_{n\in\mathbb{N}}$ defined as follows;

$$\begin{array}{lcl} G_1^*(x,A) & = & T_1(x,A) \to T_2(x,A) \to \cdots \to T_{\alpha_1}(x,A); \\ G_2^*(x,A) & = & T_1(x,U_1) \to T_2(x,U_1) \to \cdots \to T_{\alpha_2}(x,U_1); \\ & . & \\ & . & \\ & . & \\ G_{n+1}^*(x,A) & = & T_1(x,U_{n-1}) \to T_2(x,U_{n-1}) \to \cdots \to T_{\alpha_n}(x,U_{n-1}); \\ & . & \\ & . & \\ & . & \end{array} \tag{5.4}$$

where $U_1 = T_{\alpha_1}(x,A)$ and $U_n = T_{\alpha_n}(x,U_{n-1})$ for all $n \geq 2$. Are all the terms of the chain $L^x(A)$ distinct? The following theorem answers this question in the negative.

Theorem 57 *For each $k-$perfect number x, $A \in C(\Gamma_x)$; $L^x(A)$ is recurrent, in the sense that $\exists m,k \in \mathbb{N}$ such that for every $r \in \mathbb{N}\cup\{0\}$, $G_m^*(x,A) = G_{m+kr}^*(x,A)$.*

Proof. Let $n \in \mathbb{N}, A \in C(\Gamma_x)$. By definition, $G^*_{n+1}(x,A) = T_1(x,U_{n-1}) \to T_2(x,U_{n-1}) \to \cdots \to T_{\alpha_n}(x,U_{n-1})$; where $U_1 = T_{\alpha_1}(x,A)$ and $U_n = T_{\alpha_n}(x,U_{n-1})$ for all $n \geq 2$. Suppose for every $i,j \in \mathbb{N}, G^*_i(x,A) \neq G^*_j(x,A)$ whenever $i \neq j$. This means that, in particular, if $i \geq 2$ then for every $k < i, T_1(x,U_k) \neq T_1(x,U_i)$. Therefore, $\cup_{j\in\mathbb{N}} T_1(x,U_i)$ must be an infinite set. We have a contradiction, since $C(\Gamma_x)$ is finite and $\cup_{j\in\mathbb{N}} T_1(x,U_i) \subset C(\Gamma_x)$. So, $L^x(A)$ must be recurrent. ∎

In the sequence $L^x(A)$, let $G^*_m(x,A)$ be the first term satisfying $G^*_m(x,A) = G^*_r(x,A)$ for some $r \in \mathbb{N}, A \in C(\Gamma_x), r > m$. Set

$$m_r = \min\left\{y \in \mathbb{N} : y > m, G^*_m(x,A) = G^*_y(x,A)\right\}$$

and define

$$T^x_*(A) = \bigcup_{\substack{a \in G^*_k(x,A) \\ m \leq k < m_r}} a \text{ and } \lambda = \prod_{y \in T^x_*(A)} y. \tag{5.5}$$

Proof. (Theorem 55): (i) Suppose $\sigma(x) = kx, k$ prime and $T^x_*(A) \neq \Gamma_x$. Set $B = \Gamma_x \backslash T^x_*(A)$. So B is non-empty. Now, we have $\sigma\left(\prod_{z\in B} z\right) = g\prod_{z\in B} z$, where $g > 1, g|\lambda\left(\lambda = \prod_{y\in T^x_*(A)} y\right)$ or $g|k$. We must have $g = k$; since $\sigma\left(\prod_{z\in B} z\right) = \prod_{z\in B} z$ is impossible and k is prime. But then, this would mean that $\sigma\left(\prod_{z\in T^x_*(A)} z\right) = \prod_{z\in T^x_*(A)} z$ which is impossible. Therefore, B cannot be non-empty.

(ii) Clearly, if $B = \Gamma_x \backslash T^x_*(A) \neq \varnothing$ then $\prod_{z\in B} z$ divides $\sigma\left(\prod_{z\in B} z\right)$ and since $\sigma\left(\prod_{z\in B} z\right) > \prod_{z\in B} z$; the result follows. ∎

5.1.1 $k-$perfect numbers and completely multiplicative functions

We will use lemma 58 to produce necessary conditions for a positive integer to be a $k-$ perfect number. This is a new approach in our study of OPNs and since we can define many distinct multiplicative functions, this approach gives us a great deal of flexibility in dealing with the problem. In lemma 59, 60 we give some examples.

Lemma 58 *A positive integer x is a $k-$perfect number if and only if for every completely-multiplicative function $f : \mathbb{N} \longrightarrow \mathbb{Z}$, we have $f(\sigma(x)) = f(kx)$.*

The proof is clear.

Lemma 59 *If p is prime such that $p \equiv 1, 3, 5, 7$ or $9 \pmod{10}$ then $\forall m \in \mathbb{N}$,*

$$p^{2m} \equiv \begin{cases} 9, & \text{if } m \text{ is odd, } p \equiv 3 \text{ or } 7 \pmod{10} \\ 1, & \text{if } m \text{ is even, } p \equiv 3 \text{ or } 7 \pmod{10} \\ 1, & \text{if } m \in \mathbb{N},\ p \equiv 1 \text{ or } 9 \pmod{10} \\ 5, & \text{if } m \in \mathbb{N},\ p \equiv 5 \pmod{10} \end{cases} \tag{5.6}$$

and $p^{4m+1} \equiv p \pmod{10}$.

Proof. Let $p \equiv 5 \pmod{10}$. Suppose for some $k \in \mathbb{N}$, $p^{2k} \equiv 5 \pmod{10}$ then we have $p^{2(k+1)} = p^{2k}.p^2 \equiv 25.5 \pmod{10} \equiv 5 \pmod{10}$ and so $p^{2m} \equiv 5 \pmod{10}\, \forall m \in \mathbb{N}$.

If $p \equiv 1 \pmod{10}$ then clearly $p^k \equiv 1 \pmod{10}\, \forall k \in \mathbb{N}$ and so in particular $p^{2m} \equiv 1 \pmod{10}\, \forall m \in \mathbb{N}$. If $p \equiv 9 \pmod{10}$ then $p^2 \equiv 1 \pmod{10}$ and so for every $m \in \mathbb{N}, p^{2m} = (p^2)^m \equiv 1 \pmod{10}$. $p \equiv 3 \pmod{10} \Longrightarrow p^2 \equiv 9 \pmod{10}$ and $p^4 \equiv 1 \pmod{10}$. Therefore, if m is even then $p^{2m} \equiv p^{4r} \pmod{10}$ for some $r \in \mathbb{N}$ and so $p^{2m} \equiv 1 \pmod{10}$. Similarly, $p \equiv 7 \pmod{10} \Longrightarrow p^2 \equiv 9 \pmod{10}$ and for every m even, $p^{2m} \equiv 1 \pmod{10}$. The case $p^{2m} \equiv 9 \pmod{10}$ if $p \equiv 3$ or $7 \pmod{10}$ follows from the arguments above.

Now, using the results above, we have

$$p^{4m+1} = p^{4m}.p \equiv \begin{cases} 1.p, & \text{if } p \equiv 1, 3, 7 \text{ or } 9 \pmod{10} \\ 5, & \text{if } p \equiv 5 \pmod{10} \end{cases},$$

hence, $p^{4m+1} \equiv p \pmod{10}\, \forall m \geq 0$. ∎

In the same vein it is easy to verify the following statement.

Lemma 60 *Let p be a prime. If*

(i) $p \equiv 1 \pmod{10}$ *then* $\forall m \in \mathbb{N}, \sigma(p^{2m}) \equiv 1, 3, 5, 7$ *or* $9 \pmod{10}$*;*
(ii) $p \equiv 3 \pmod{10}$ *then* $\forall m \in \mathbb{N}, \sigma(p^{2m}) \equiv 1$ *or* $3 \pmod{10}$*;*
(iii) $p \equiv 5 \pmod{10}$ *then* $\forall m \in \mathbb{N}, \sigma(p^{2m}) \equiv 1 \pmod{10}$*;*
(iv) $p \equiv 7 \pmod{10}$ *then* $\forall m \in \mathbb{N}, \sigma(p^{2m}) \equiv 1$ *or* $7 \pmod{10}$*;*
(v) $p \equiv 9 \pmod{10}$ *then* $\forall m \in \mathbb{N}, \sigma(p^{2m}) \equiv 1 \pmod{10}$*;*
(vi) $p \equiv 1 \pmod{10}$ *then* $\forall m \geq 0, \sigma(p^{4m+1}) \equiv 2, 4, 6, 8$ *or* $0 \pmod{10}$*;*
(vii) $p \equiv 3 \pmod{10}$ *then* $\forall m \geq 0, \sigma(p^{4m+1}) \equiv 4 \pmod{10}$*;*
(viii) $p \equiv 5 \pmod{10}$ *then* $\forall m \geq 0, \sigma(p^{4m+1}) \equiv 6 \pmod{10}$*;*
(ix) $p \equiv 7 \pmod{10}$ *then* $\forall m \geq 0, \sigma(p^{4m+1}) \equiv 8 \pmod{10}$*;*
(x) $p \equiv 9 \pmod{10}$ *then* $\forall m \geq 0, \sigma(p^{4m+1}) \equiv 0 \pmod{10}$.

For the rest of this section, the expression $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ represents an odd integer that satisfies the conditions $p \equiv \alpha \equiv 1 \pmod{4}$ where p is prime, $p^{\alpha} || N$ and $q_1, q_2, ..., q_k$ are distinct primes. Define

$$R_k(N) = \{q_1, q_2, ..., q_k\}. \tag{5.7}$$

We will now give some necessary conditions for N to be an OPN.

Theorem 61 *If $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN and $5|N$ then either (i)$p \equiv 1$ or $9 \pmod{10}$ or (ii) $q_i \equiv 1 \pmod{10}$ and $r_i = 5m + 2$ for some $m \geq 0, i\,(1 \leq i \leq k)$.*

Proof. Let $f_{10} : \mathbb{N} \longrightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be a function satisfying $f_{10}(x) \equiv x \pmod{10}, \forall x \in \mathbb{N}$ then it is clear that f_{10} is completely multiplicative. Therefore, by lemma 58, $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN if and only if

$$f_{10}\left(2p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}\right) = f_{10}\left(\sigma(p^{\alpha})\,\sigma\left(q_1^{2r_1}\right) ... \sigma\left(q_k^{2r_k}\right)\right). \tag{5.8}$$

We want to show that if $5|N$ and the statement in (5.8) holds then (i) $p \equiv 1$ or $9 \pmod{10}$ or (ii) $q_i \equiv 1 \pmod{10}$ and $r_i = 5m + 2$ for some $m \geq 0, i\,(1 \leq i \leq k)$.

Suppose that $5|N$. If $5|p$ then $5|\sigma\left(q_i^{2r_i}\right)$ for some $i\,(1 \leq i \leq k)$. From lemma 54, we must have $q_i \equiv 1 \pmod{10}$ since for every prime s, and every positive integer $m, 5|\sigma\left(s^{2m}\right) \Longrightarrow s \equiv 1 \pmod{10}$.

Now $\sigma\left(s^{2k}\right) \equiv 1, 3, 5, 7$ or $9 \pmod{10}, \forall k \in \mathbb{N}$. Furthermore,

$\sigma\left(s^2\right) \equiv 3 \pmod{10}$, so $5 \nmid \sigma\left(s^2\right)$;

$\sigma\left(s^4\right) \equiv 5 \pmod{10}$, so $5|\sigma\left(s^4\right)$;

$\sigma\left(s^6\right) \equiv 7 \pmod{10}$, so $5 \nmid \sigma\left(s^6\right)$;

$\sigma\left(s^8\right) \equiv 9 \pmod{10}$, so $5 \nmid \sigma\left(s^8\right)$;

$\sigma\left(s^{10}\right) \equiv 1 \pmod{10}$, so $5 \nmid \sigma\left(s^{10}\right)$;

$\sigma\left(s^{12}\right) \equiv 3 \pmod{10}$, so $5 \nmid \sigma\left(s^{12}\right)$.

Continuing in this way, we have for every $m \geq 0$

$$\sigma\left(s^{2(5m+r)}\right) \equiv \begin{cases} 1 \pmod{10}, & \text{if } r = 0 \\ 3 \pmod{10}, & \text{if } r = 1 \\ 5 \pmod{10}, & \text{if } r = 2 \\ 7 \pmod{10}, & \text{if } r = 3 \\ 9 \pmod{10}, & \text{if } r = 4 \end{cases}. \tag{5.9}$$

Therefore, $r_i = 5m + 2$ for some $m \geq 0, i\,(1 \leq i \leq n)$. If $5 \nmid p$ and $5 \nmid \sigma\left(q_i^{2r_i}\right)$ for every i then we must have $5|\sigma\left(p^\alpha\right)$. By lemma 58, this can occur only if $p \equiv 1$ or $9 \pmod{10}$. This completes the proof. ∎

We can apply lemma 58 to the cases where $p \equiv 1$ or $3 \pmod{4}$. The following result is easy to check.

Lemma 62 *If p is prime such that $p \equiv 1$ or $3 \pmod{4}$ then $\forall m \in \mathbb{N}$,*

$$p^{2m} \equiv \begin{cases} 1, & \text{if } m \in \mathbb{N},\ p \equiv 1 \pmod{4} \\ 3, & \text{if } m \text{ is odd},\ p \equiv 3 \pmod{4} \\ 1, & \text{if } m \text{ is even},\ p \equiv 3 \pmod{4} \end{cases} \tag{5.10}$$

and $p^{4m+1} \equiv p \pmod{4}\, \forall m \geq 0$. Furthermore, we have

$$\sigma\left(p^{2m}\right) \equiv \begin{cases} 1, & \text{if } m \text{ is even},\ p \equiv 1 \pmod{4} \\ 3, & \text{if } m \text{ is odd},\ p \equiv 1 \pmod{4} \\ 1, & \text{if } m \text{ is even},\ p \equiv 3 \pmod{4} \\ 3, & \text{if } m \text{ is odd},\ p \equiv 3 \pmod{4} \end{cases} \tag{5.11}$$

and

$$\sigma\left(p^{4m+1}\right) \equiv \begin{cases} 2, & \text{if } m \geq 0,\ p \equiv 1 \pmod 4 \\ 0, & \text{if } m \geq 0,\ p \equiv 3 \pmod 4 \end{cases} \tag{5.12}$$

For every $n \in \mathbb{N}$, $f_k : \mathbb{N} \longrightarrow \mathbb{Z}$ will always represent a function satisfying $f_k(x) \equiv k \pmod{\text{n}}, \forall x \in \mathbb{N}$. Now, we can apply lemma 62 to prove the following theorem.

Theorem 63 *If $N = p^{\alpha} q_1^{2r_1} q_2^{2r_2} ... q_k^{2r_k}$ is an OPN then $T \equiv 0$ or $1 \pmod 4$ where*

$$T = \left|\{i | 1 \leq i \leq k, r_i \text{ odd}, q_i \equiv 1 \pmod 4\}\right|.$$

Proof. Write

$$N = p^{\alpha}. \prod_{a \in A} a^{v_a(N)}. \prod_{b \in B} b^{v_b(N)}. \prod_{c \in C} c^{v_c(N)}. \prod_{d \in D} d^{v_d(N)} \tag{5.13}$$

where
$A = \left\{x \in R_k(N) | x \equiv 1 \pmod 4, \frac{v_x(N)}{2} \text{ is even}\right\}$;
$B = \left\{x \in R_k(N) | x \equiv 1 \pmod 4, \frac{v_x(N)}{2} \text{ is odd}\right\}$;
$C = \left\{x \in R_k(N) | x \equiv 3 \pmod 4, \frac{v_x(N)}{2} \text{ is even}\right\}$;
$D = \left\{x \in R_k(N) | x \equiv 3 \pmod 4, \frac{v_x(N)}{2} \text{ is odd}\right\}$
and for every $a \in \mathbb{N}, p$ prime;

$$v_p(a) = \max\{r \in \mathbb{N} : p^r || a\} \tag{5.14}$$

N is an OPN if and only if $f_4\left(2p^{\alpha}. \prod_{a \in A} a^{v_a(N)}. \prod_{b \in B} b^{v_b(N)}. \prod_{c \in C} c^{v_c(N)}. \prod_{d \in D} d^{v_d(N)}\right)$
$= f_4\left(\sigma\left(p^{\alpha}. \prod_{a \in A} a^{v_a(N)}. \prod_{b \in B} b^{v_b(N)}. \prod_{c \in C} c^{v_c(N)}. \prod_{d \in D} d^{v_d(N)}\right)\right)$. Now
$f_4\left(2p^{\alpha}. \prod_{a \in A} a^{v_a(N)}. \prod_{b \in B} b^{v_b(N)}. \prod_{c \in C} c^{v_c(N)}. \prod_{d \in D} d^{v_d(N)}\right)$
$\equiv f_4(2). f_4(p^{\alpha}). f_4\left(\prod_{a \in A} a^{v_a(N)}\right). f_4\left(\prod_{b \in B} b^{v_b(N)}\right). f_4\left(\prod_{c \in C} c^{v_c(N)}\right)$
$f_4\left(\prod_{d \in D} d^{v_d(N)}\right)$

$\equiv 2.1.1.1.3^{|D|} \equiv 2\left(3^{|D|}\right)$. Similarly,

$f_4\left(\sigma\left(p^{\alpha}.\prod_{a\in A}a^{v_a(N)}.\prod_{b\in B}b^{v_b(N)}.\prod_{c\in C}c^{v_c(N)}.\prod_{d\in D}d^{v_d(N)}\right)\right)$

$\equiv f_4\left(\sigma\left(p^{\alpha}\right)\right).f_4\left(\sigma\left(\prod_{a\in A}a^{v_a(N)}\right)\right).f_4\left(\sigma\left(\prod_{b\in B}b^{v_b(N)}\right)\right).f_4\left(\sigma\left(\prod_{c\in C}c^{v_c(N)}\right)\right)$

$.f_4\left(\sigma\left(\prod_{d\in D}d^{v_d(N)}\right)\right) \equiv 2.1.3^{|B|}.1.3^{|D|} \equiv 2\left(3^{|B|}\right)\left(3^{|D|}\right)$. From the expressions, $2\left(3^{|D|}\right)$ and $2\left(3^{|B|}\right)\left(3^{|D|}\right)$ it is clear that we must have $3^{|B|} \equiv 1$ or $3 \pmod 4$. This implies that $|B| \equiv 0$ or $1 \pmod 4$ and the proof is complete since $B = T$. ∎

It is possible to use different completely multiplicative functions in the application of lemma 58 and produce new results for N to be an OPN. For now, theorem 62 and 63 are important new statements concerning the existence of odd perfect numbers.

5.2 On the set of divisors of a positive non perfect square x. $L(x), L^d(x)$ and $L^u(x), x \in \mathbb{N}$.

It is known that no perfect number is a perfect square. Therefore, we considered the sets; $L(x), L^d(x)$ and $L^u(x), x \in \mathbb{N}$, x is not a perfect square. These sets are defined as follow:

(i) $L(x) = \{y \in \mathbb{N} : y|x\}$,

(ii) $L^d(x) = \{y \in L(x) : y < \sqrt{x}\}$ and

(iii) $L^u(x) = \{y \in L(x) : y > \sqrt{x}\}$.

So, by definition, we should have $L(x) = L^d(x) \cup L^u(x), x \in \mathbb{N}$, x is not a perfect square.

Suppose $x \in \mathbb{N}$ is a positive non perfect square, so that $L(x) = L^d(x) \cup L^u(x)$. Write $L^d(x) = \{x_d(i) : 1 \leq i \leq n_x, x_d(1) < x_d(2) < \cdots < x_d(n_x)\}$

and $L^u(x) = \{x_u(i) : 1 \leq i \leq n_x, x_u(1) > x_u(2) > \cdots > x_u(n_x)\}$ where n_x is half the number of elements in $L(x)$. So, for each $j\,(1 \leq j \leq n_x)$,

$x_d(j)\,x_u(j) = x$. Note that for a given x, it may be possible to find another positive integer y such that $L^d(x) = L^d(y)$. So, whether x or y is a perfect number will depend on $L^d(x)\,\big(= L^d(y)\big)$. Furthermore, if $L^d(x) = L^d(y)$ then for each $j\,(1 \leq j \leq n_x)$, $x_d(j)\,x_u(j) = x$ and $x_d(j)\,y_u(j) = y$, since $x_d(j) = y_d(j)$. It is easy to see that

$$\sum_{j=2}^{n_x} \frac{x}{x_d(j)} = \sum_{j=2}^{n_x} x_u(j). \tag{5.15}$$

If we write

$$\sum_{j=2}^{n_x} \frac{1}{x_d(j)} = \frac{g_x}{\mathrm{lcm}\left(\mathrm{x_d}(1), \mathrm{x_d}(2), ..., \mathrm{x_d}(\mathrm{n_x})\right)} \tag{5.16}$$

for some $g_x \in \mathbb{N}$, where $\mathrm{lcm}\left(\mathrm{x_d}(1), \mathrm{x_d}(2), ..., \mathrm{x_d}(\mathrm{n_x})\right)$ is the least common multiple of the elements $x_d(1), x_d(2), ..., x_d(n_x)$ then we have

$$1 - \sum_{j=2}^{n_x} \frac{1}{x_d(j)} = \frac{h_x}{\mathrm{lcm}\left(\mathrm{x_d}(1), \mathrm{x_d}(2), ..., \mathrm{x_d}(\mathrm{n_x})\right)} \tag{5.17}$$

for some $h_x \in \mathbb{N}$. Now, a positive integer y, not a perfect square, with $L^d(x) = L^d(y)$, is perfect if

$$\begin{aligned} y\left(1 - \sum_{j=2}^{n_x} \tfrac{1}{x_d(j)}\right) &= y - \sum_{j=2}^{n_x} \tfrac{y}{x_d(j)} \\ &= y - \sum_{j=2}^{n_x} y_u(j) \\ &= \sum_{j=1}^{n_x} y_d(j). \end{aligned}$$

This shows why investigating this object, $1 - \sum_{j=2}^{n_x} 1/x_d(j)$ closely, can help us identify many positive integers that cannot be a perfect number. For example, consider $A = \{1, 3, 9\}$. Clearly, there are infinitely-many positive integers y such that $L^d(y) = \{1, 3, 9\}$. Can any of these integers be a perfect number? The answer is no. To see this notice that if y is perfect then $y\,(1 - (1/3 + 1/9)) = 1 + 3 + 9$. This is impossible since there is no positive integer y such that $(5/9)\,y = 13$. It also means that no integer of the form $9p$, p a prime, is perfect.

We stated that it is possible to find infinitely-many positive integers $y_1 < y_2 < \cdots$ such that $L^d(y_1) = L^d(y_j), j \in \mathbb{N}$. Now, if y_1 is perfect, can y_j be perfect for some $j \in \mathbb{N}, j > 1$?

Lemma 64 *(a) Let $y_j, j \in \mathbb{N}$ be positive integers satisfying $y_1 < y_2 < \cdots$ such that $L^d(y_i) = L^d(y_j), i, j \in \mathbb{N}$ then*

(i) if y_i is deficient then y_{i+1} is deficient;

(ii) if y_i is perfect then y_{i+1} is deficient;

(iii) if y_i is abundant then y_{i+1} is abundant, deficient or perfect.

(b) Let x be a perfect number. If $x_u(n_x)$ is prime then

(i) $x_u(n_x) | y$, for every $y \in L^u(x)$ and

(ii) $x_u(n_x) = \sum_{c \in L^d(x)} c$, where $n_x = |L^u(x)| = \left|L^d(x)\right|$.

Proof. (a) Write $y = y_i$, $z = y_{i+1}$. (i) y deficient means

$$y\left(1 - \sum_{j=2}^{n_y} \frac{1}{y_d(j)}\right) > \sum_{j=1}^{n_y} y_d(j)$$

and since $z > y$ and $L^d(y) = L^d(z)$ we must have $z\left(1 - \sum_{j=2}^{n_y} 1/y_d(j)\right) > \sum_{j=1}^{n_y} y_d(j)$ and the result follows, z is deficient. In similar fashion, one can prove (ii) and (iii).

(b) (i) $\gcd(x_u(n_x), x_d(n_x)) = 1$ since $x_u(n_x)$ is prime. Therefore, $x_u(n_x) | y$, for every $y \in L^u(x)$.

(ii) Since $\gcd(x_u(n_x), x_d(n_x)) = 1$, $a | x_d(n_x), \forall a \in L^d(x)$ and so $\sigma(x_d(n_x)) = \sum_{s \in L^d(x)} s$. From (i), $\sum_{s \in L^u(x)} s = k x_u(n_x)$,for some $k \in \mathbb{N}$, and so $x_u(n_x) \mid \sum_{s \in L^d(x)} s$. We need to show that if $\sum_{s \in L^d(x)} s = g x_u(n_x)$ for some $g \in \mathbb{N}$, then $g = 1$. Suppose $\sum_{s \in L^d(x)} s = g x_u(n_x)$ for some $g \in \mathbb{N}$, and $g > 1$, then

$$\sigma(x_d(n_x)) = \sum_{s \in L^d(x)} s = g x_u(n_x) \geq 2 x_u(n_x) > 2 x_d(n_x).$$

This implies that $x_d(n_x)$ is abundant which is not possible since every proper divisor of a perfect number must be deficient and so we have a contradiction. Therefore, $x_u(n_x) = \sum_{s \in L^d(x)} s$. ▪

We now give different proofs of our first statement concerning the existence of a prime in $L^u(x), x \in \mathbb{N}$, x a non-perfect square.

Theorem 65 *Let x be a perfect number. Then $L^u(x)$ contains a prime number if and only if $x_d(n_x)$ is a power of 2.*

Proof. Suppose $x_d(n_x) = 2^y$ for some positive integer y. Then $x_u(n_x)$ must be a prime since no power of 2 is a perfect number.

Conversely, suppose $x_u(n_x)$ is prime, then $x_u(n_x) = \sum_{s \in L^d(x)} s$. Therefore, suppose that $x_d(n_x) = \prod_{i=1}^{n} p_i^{r_i}$ for some positive integers $r_1, r_2, ..., r_n\ (n > 1)$ and distinct primes $p_1, p_2, ..., p_n$. We have $\sigma(x_d(n_x)) = \sum_{s \in L^d(x)} s$ since $x_u(n_x)$ is prime. But

$$\sigma(x_d(n_x)) = \sum\nolimits_{s \in L^d(x)} s = \prod_{i=1}^{n} \frac{p_i^{r_i} - 1}{p_i - 1} = x_u(n_x)$$

is not possible if all the primes are distinct, odd and $n > 1$. Therefore, $p_i = 2$ for all $i\ (1 \leq i \leq n)$ and the result follows. ▪

The following theorems are a direct consequence of theorem 65.

Theorem 66 *(Acquaah P. [1]) The largest prime divisor of an odd perfect number g is less than $g^{1/2}$.*

Theorem 67 *If g is an odd perfect number and p^u is a prime power divisor of g then $p^u < \sqrt{g}$.*

Proof. (theorem 67) If $n = p^\alpha \lambda^2$ is an odd perfect number, where $p \equiv \alpha \equiv 1 \pmod 4$ and $\gcd(p^\alpha, \lambda^2) = 1$ then we know that $\sigma(\lambda^2) = p^\alpha$ and $\sigma(p^\alpha) = 2\lambda^2$ is impossible. So, let g be an odd perfect number and write $g = p^u n$, where p is prime, $p^u || g$ and $\gcd(p^u, n) = 1$. We claim that $p^u < \sqrt{g}$. Since

g is perfect, we have $\sigma(g) = 2g = 2p^u n = \sigma(p^u)\sigma(g)$ and $\gcd(p^u, \sigma(p^u)) = 1$ means $p^u | \sigma(n)$. Furthermore, since $\sigma(n) < 2n$, we have $p^u | \sigma(n) \Rightarrow p^u = \sigma(n)$ or $p^u < n$. We show that $p^u = \sigma(n)$ is impossible.

Case 1: p is the special prime. In this case $p^u = \sigma(n)$ implies that $\sigma(p^u) = 2n$, since g is perfect. That is, g must satisfy the conditions $p^u = \sigma(n)$ and $\sigma(p^u) = 2n$. But this is impossible.

Case 2: p is not the special prime. Here, $p^u = \sigma(n)$ is impossible since n is divisible by q^λ, where q is the special prime, $q \equiv \lambda \equiv 1 \pmod 4$ and $q^\lambda || n$. Therefore, $\sigma(n)$ is even. However, p^u is odd. Hence, in both cases, $p^u = \sigma(n)$ is impossible. Therefore, $p^u < n$.

Conclusion: Since, $p^u < n$ and $g = p^u n$, we have $p^u < \sqrt{g}$. Furthermore, since $p^u || g$ and p^u is any prime power divisor of g, we have that every prime power divisor of g is less than $\sqrt{g}$. ▪

This means that if g is an odd perfect number then the set $L^u(g)$ contains no prime-power divisor of g. We can then state the following theorem about the nature of the set $L^d(g)$, g an odd perfect number.

Theorem 68 *If x is an OPN then* $\mathrm{lcm}(\mathrm{x_d}(1), \mathrm{x_d}(2), ..., \mathrm{x_d}(\mathrm{n_x})) = \mathrm{x}$.

Theorem 68 shows that every prime-power of an odd perfect number x belongs to the set $L^d(x)$. We can extend this idea as follows. First, if x is a perfect number then there must be some pair of positive integers (A, B) such that $x = AB, \gcd(A, B) = 1, \gcd(A, \sigma(A)) = 1$ and $2|\sigma(B)$. In the case of even perfect numbers we have $x = 2^{p-1}(2^p - 1)$ for some prime p. So we can choose $A = 2^{p-1}$ and $B = 2^p - 1$. If x is an OPN, then any of the non special-prime powers $q_i^{2r_i} || x$ can be chosen for A and $x/q_i^{2r_i}$ for B.

Theorem 69 *Let x be a perfect number. If $x = AB, \gcd(A, B) = 1$, $\gcd(A, \sigma(A)) = 1$ and $2|\sigma(B)$ for some pair of positive integers (A, B), then $A \in L^d(x)$.*

Proof. Let $x = AB, \gcd(A, B) = 1, \gcd(A, \sigma(A)) = 1$ and $2|\sigma(B)$ for some pair of positive integers (A, B). $2|\sigma(B) \Longrightarrow \sigma(B) = 2B - e$ for some positive

even integer e. Therefore, $\sigma(A) = 2A - u$ for some positive odd integer u. x perfect implies that $2x = 2AB = \sigma(AB) = \sigma(A)\sigma(B) = (2A-u)(2B-e)$. Therefore,

$$2A/u = (2B-e)/(B-e). \tag{5.18}$$

Now, $\gcd(A, \sigma(A)) = 1 \Longrightarrow \gcd(2A, u) = 1$. So, we have $2B - e = 2Ak, B - e = uk$ for some positive integer k. From (5.18), we have $\sigma(B) = 2Ak$, that is $2A|\sigma(B)$ which implies that $2A = \sigma(B)$ or $2A < B$. $2A < B \Longrightarrow A < B/2 \Longrightarrow A < B$. $2A = \sigma(B) \Longrightarrow A|\sigma(B) \Longrightarrow A = \sigma(B)$ or $A < B$. Therefore, $A < B$ since $A = \sigma(B)$ is impossible. This completes the proof. ▪

We give another proof of theorem 66 below. This time we apply Hagis [22], Kishore [33] and Nielsen [40]. If n is an OPN then it has at least 9 distinct prime divisors.

Proof. (Theorem 66) Given g is an odd perfect number, it must be of the form $g = p^{4k+1}n^2 = p^{4k+1}\prod_{i=1}^{m} q_i^{2t_i}$ where $m \in \mathbb{N}, m > 8, \gcd(p, n) = 1, \prod_{i=1}^{m} q_i^{2t_i}$ is the prime factorization of n^2 and $p \equiv 1 \pmod 4$. The theorem follows easily if $k \neq 0$ since every divisor of g is less than $\sqrt{p^{4k+1}n^2} = \sqrt{p^{4k+1}}\prod_{i=1}^{m} q_i^{t_i}$. If $k = 0$, then $q_i < \sqrt{g}$ for all i and since g is a perfect number, we must have

$$2g = \sigma(p)\prod_{i=1}^{m}\sigma\left(q_i^{2t_i}\right).$$

Therefore, p must divide $\prod_{i=1}^{m}\sigma\left(q_i^{2t_i}\right)$ and since $m > 8, p(p+1)d = 2g$ for some $d > 2$; completing the proof. ▪

Theorem 66 was improved in P. Acquaah and S. Kongayin [2]; this result restricts the size of the largest prime divisor of an odd perfect number g.

Theorem 70 *(Acquaah P., Konyagin S.[2]) The largest prime divisor of an odd perfect number g is less than $(3g)^{1/3}$.*

Proof. p, q will denote primes.

If p is an odd prime and r a positive integer then $\sigma(p^r) = \frac{p^{r+1}-1}{p-1} < 3p^r/2$. If $x, r \in \mathbb{N}, q^r||x$ and $r \geq 2$,then $2x = \sigma(x)$ is divisible by $q^r\sigma(q^r) > q^{2r} \geq q^4$. Hence, $q < (2x)^{1/4}$and we are done.

If x is an odd perfect number then we know that $x = Q^\alpha m^2$ for some prime Q, positive integers α, m satisfying $Q \equiv \alpha \equiv 1 \pmod 4, \gcd(Q, m) = 1$. If $q|x$ and $q \neq Q$ then $q^2|x$. So to prove the theorem, we suppose that $q \neq Q$.

Since x is perfect, there is a prime power $p^{2a}||x$ with $q|\sigma(p^{2a})$. Write x as $qp^{2a}v^2$. We consider two cases. Suppose that $p|\sigma(q)$. In this case we follow the arguments from [38]. We have $qp^{2a}||\sigma(p^{2a}v^2)$. Thus,

$$2x = \sigma(x) = (q+1)\,\sigma\left(p^{2a}v^2\right) > p^{2a}q^2 > \frac{2q^2\sigma(p^{2a})}{3} > \frac{2q^3}{3},$$

and we are done.

Now suppose that $p|\sigma(q)$. Denote $u \equiv \sigma(p^{2a})/q$. Since

$$\sigma\left(p^{2a}\right) \equiv 1 \pmod{\text{p}}, q \equiv \pmod{\text{p}},$$

we conclude that $u \equiv -1 \pmod{\text{p}}$. Moreover, $u \neq p-1$ since u is odd. Thus,

$$u \geq 2p - 1. \tag{5.19}$$

Let $p^b||\sigma(q)$. By our supposition, $b \geq 1$. We notice that $p^{2a-b}||\sigma(v^2)$. Therefore, $b \leq 2a$ and also

$$\sigma\left(v^2\right) \geq p^{2a-b}. \tag{5.20}$$

We have

$$p^{2a+1} - 1 = (p-1)\,\sigma\left(p^{2a}\right) = (p-1)\,uq = (p-1)\,u\sigma(q) - (p-1)\,u.$$

Therefore, $(p-1)\,u \equiv 1 \pmod{\text{p}^{\text{b}}}$. Thus,

$$(p-1)\,u > p^b.$$

Combining this inequality with (5.20), we get

$$u\sigma\left(v^2\right) > \frac{p^{2a}}{p-1}. \tag{5.21}$$

Now we have

$$2x = \sigma(x) = \sigma(q)\,\sigma\left(p^{2a}\right)\sigma\left(v^2\right) = (q+1)\,uq\sigma\left(v^2\right).$$

Next, by (5.19) and (5.21),

$$2x > p^{2a}q^2/(p-1) > \frac{2\sigma\left(p^{2a}\right)q^2}{3(p-1)} = \frac{2uq^3}{3(p-1)} \geq \frac{2(2p-1)q^3}{3(p-1)} > \frac{4q^3}{3}.$$

So, $x > 2q^3/3$. This completes the proof. ∎

Chapter 6

Summary and Conclusion

It is known that there are infinitely-many primes in the sequence $an+b$, whenever $a, b \in \mathbb{N}$ and $\gcd(a,b) = 1$. We provided an alternate proof of this celebrated theorem by applying a basic sieve result. G.H. Hardy and J.E. Littlewood [25] gave the following conjecture for the sequence $an^2 + bn + c$.

Conjecture 71 *Suppose a, b and c are integers with $a > 0, \gcd(a,b,c) = 1, a+b$ and c are not both even, and $D = b^2 - 4ac$ is not a square. Let $P_f(x)$ be the number of primes $p \leq x$ of the form $p = f(n) = an^2 + bn + c, n \in \mathbb{Z}$. Then*

$$P_f(x) \sim \gcd(2, a+b) \frac{g(D)}{\sqrt{a}} \frac{\sqrt{x}}{\log x} \prod_{\substack{p|a, p|b \\ p>2}} \frac{p}{p-1} \tag{6.1}$$

where

$$g(D) = \prod_{\substack{p \nmid a \\ p>2}} \left(1 - \frac{\left(\frac{D}{p}\right)}{p-1}\right) \tag{6.2}$$

and $\left(\frac{D}{p}\right)$ is the Legendre's symbol.

This conjecture is unsolved and it is not even known if there is a polynomial of degree two or higher that admits infinitely many primes. A. Schinzel

and W. Sierpiński [48] also conjectured that if f is an irreducible polynomial(of any degree) with integer coefficients that is not congruent to zero modulo any prime, then $f(n)$ is prime for infinitely many integers n.

The method we used in proving Dirichlet's theorem cannot be used, in its current form, to attack this type of problem. The following theorem is also a beautiful connection between cyclotomic polynomials and primes of the form $an+1$.

Theorem 72 *For every positive integer a, there are infinitely-many primes of the form $an+1$.*

Proof: If $a=1$, the result is trivial. So assume $a>1$ and there are finitely many primes $p_1<\cdots<p_k$ with $p_i\equiv 1\,(\text{mod a}),1\leq i\leq k$. Let $G=p_1...p_k$ then $G>1$ and so we can find r large enough so that $\Phi_a(G^r)>1$. If s is a prime divisor of $\Phi_a(G^r)$ then since $s|G^{ra}-1$, we have $s\nmid G$. So s is not of the form $an+1$ and s$\nmid a$. This contradicts (i) of theorem 52. Therefore, there are infinitely many primes of the form $an+1$.■

We introduce the following basic arithmetic function λ_* and we believe, from current developments, that a modification of the methods used in this thesis, λ_* and a new promising technique can help us gain new insights in problems related to conjecture 71.

6.1 The function λ_*

Let $n\in\mathbb{N}$. Define $g_*(n)=\{n/p:p \text{ prime}\}\cup\{1\}$ and

$$\lambda_*(n)=\max g_*(n)\cap\mathbb{N}. \tag{6.3}$$

λ_* is not a multiplicative arithmetic function since

$$\lambda_*(2)=1,\lambda_*(3)=1,\gcd(2,3)=1$$

but $\lambda_*(6)=3$. The function λ_* is interesting because of the following statement.

Theorem 73 *(i) For every* $n \in \mathbb{N}$

$$\lambda_*(n) = 1 \Longleftrightarrow n = 1 \text{ or } n \text{ is prime.}$$

(ii) For every $y, m \in \mathbb{N}$

$$\lambda_*(m) = y \Longrightarrow m \leq y^2.$$

(iii) For every $y \in \mathbb{N}, y > 1$

$$|\{z \in \mathbb{N} : \lambda_*(z) = y\}| = \begin{cases} \pi(y), & \text{if } y \text{ is prime} \\ \pi(n_y), & \text{otherwise} \end{cases}$$

where

$$n_y = \min\{p : p|y\} \tag{6.4}$$

.

Proof: (i) Suppose $n = 1$ or n is prime. $\lambda_*(1) = \max g_*(1) \cap \mathbb{N} = \max\{1\} \cap \mathbb{N} = 1$. If $n = p$, prime then $\lambda_*(p) = \max g_*(p) \cap \mathbb{N} = \max\{1\} \cap \mathbb{N} = 1$. Suppose $\lambda_*(n) = 1$ and n is not prime. Without loss of generality, suppose that n is square-free. That is $n = p_1 p_2 ... p_k$, where $p_1 < p_2 < \cdots < p_k$ are distinct primes. Then $\lambda_*(p_1 p_2 ... p_k) = \max g_*(p_1 p_2 ... p_k) \cap \mathbb{N} = p_2 ... p_k \neq 1$. This contradicts our assumption that $\lambda_*(n) = 1$. Therefore, n must be prime.

(ii) Suppose $\lambda_*(m) = y$ and $m > y^2$. Since $\lambda_*(m) = y$, we have $m = yg$ for some prime $g \leq n_y$. $g \leq n_y \Longrightarrow m = gy \leq y^2$, a contradiction.

(iii) Let $y \in \mathbb{N}, y > 1, y$ prime. Suppose $z \in \mathbb{N}$ and $\lambda_*(z) = y$ then $z = n_z y$ for some prime n_z. Since $n_z \leq y$ and n_z, y are primes, we have that for every prime $p \leq y$, $\lambda_*(py) = y$. If $u < y, z = yu$ and u is composite then $u = n_u f$ for some $f > 1$. So $z = n_u f y \Longrightarrow \lambda_*(n_u f y) = fy \neq y$. Therefore, $|\{z \in \mathbb{N} : \lambda_*(z) = y\}| = \pi(y)$ whenever y is prime.

If y is composite then $y = n_y g$ for some $g > 1$, so $\lambda_*(y) = g$ and, if p is a prime satisfying $p \leq n_y$ then $\lambda_*(pg) = g$. Therefore, $|\{z \in \mathbb{N} : \lambda_*(z) = y\}| = \pi(n_y)$ whenever y is composite.■

This function does have some interesting properties that lend themselves to the study of primes in short intervals or polynomial sequences. At first it is not exactly clear how one may use λ_* in the study of primes in short-intervals. One possible area of application will be a search for primes in intervals of the form $[kx, (k+j)\,x]; x, k, j \in \mathbb{R}^+$. We did provide alternative proofs of existing theorems about primes in the intervals $[x, 2x], [2x, 3x]$ and $[3x, 4x]$. However, our method failed to resolve the case $[4x, 5x]$.

We also considered $\lambda-$ stationary polynomials in $\mathbb{Z}[x]$ but did not resolve the general problem about the existence of $f \in \mathbb{Z}^b[x]$, if $b > 0$ and $f \in \mathbb{Z}[x]$. This problem is interesting and will be researched further. The other side of the thesis involved problems concerning the existence of odd perfect numbers. We still do not know if an odd perfect number exists and most researchers are now focused on the size of the prime divisors or lower-bounds of an odd perfect number, if it exists. Our most important result in this direction is that the largest prime divisor of an odd perfect number x must be less than $(3x)^{1/3}$. We also showed how completely-multiplicative functions can be used to derive new necessary conditions concerning OPNs may be discovered if we push this technique further.

Bibliography

[1] Acquaah P. (2013), "*An important difference between odd perfect and even perfect numbers*", Universal Journal of Mathematics and Mathematical Sciences, Volume 4, Issue 1, Pages 85 - 90.

[2] Acquaah P. and Kongayin S.(2012), "*On Prime factors of Odd Perfect Numbers*". International Journal of Number Theory: 6.1537.1540v8.

[3] Apostol, T. M (1976). "*Introduction to analytic number theory*". Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg.

[4] Apostol, T. M (1970). "*Resultants of Cyclotomic Polynomials*". Proc. Amer. Math. Soc. 24, 457-462,.

[5] Bachraoui M. El. (2006), "*Primes in the interval* $(2n, 3n)$". International Journal of Contemporary Mathematical Science. Vol. 1, , n0. 13, 617-621.

[6] Bombieri, E. (1987). "*Le Grand Crible dans la Théorie Analytique des Nombres*". Astérisque 18 (Seconde ed.). Paris. Zbl 0618.10042.

[7] Brent, R. P.; Cohen, G. L. (1989). "*A New Lower Bound for Odd Perfect Numbers*". Mathematics of Computation, Vol. 53 (187): pp. 431-437.

[8] Brun V. (1915). "*Uber das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*". Archiv for Math. og Naturvid. B 34, no. 8, 19 pp.- reported in Kelvin Ford (2004) : "On Bombieri's asymptotic sieve",

Transactions of the American Mathematical Society, Volume 357, Number 4, pages 1663-1674.

[9] Carmichael R. D. (1906- 1907), "*Multiply perfect numbers of four different primes*", Annals of Math. 8, 149158.

[10] Chebyshev P. L.(1852), "*Mémoire sur les nombres premiers.*" Journal de Math. Pures et Appl. 17, 366-390.

[11] Chen W W L (1981), "*Primes in Arithmetic Progressions.*", Chapter 4, Imperial College London. https://rutherglen.science.mq.edu.au/wchen/lndpnfolder/dpn04.pdf.

[12] Cohen G. L. (1981), "*Even perfect numbers*", Math. Gaz. 65, 2830.

[13] Dickson L. E. (1971), "*History of the theory of numbers*", vol. 1, pp. 333, Chelsea Pub. Co., New York.

[14] Dickson L. E. (1911), "*Notes on the theory of numbers*", Amer. Math. Monthly 18,109.

[15] Dickson, L. E.; Mitchell, H. H.; Vandiver, H. S.; and Wahlin, G. E (1923). "*Algebraic Numbers*". Bull Nat. Res. Council, Vol. 5, Part 3, No. 28. Washington, DC: National Acad. Sci.,.

[16] Dusart P. (1999), "*Ingalits explicites pour* $\pi(x)$,$\vartheta(x)$ *and* $\psi(x)$, *et les nombres premiers*". C.R. Math. Acad. Sci. Soc. R. Can. 21, no 2, 53-59.

[17] Erdos P. and Suranyi J. (2003) "*Topics in the theory of numbers.*" Undergraduate Texts in Mathematics. Springer Verlag, 2003. viii+287 pp.

[18] Furstenberg, H. (1955). "*On the infinitude of primes*". American Mathematical Monthly (Mathematical Association of America) 62 (5): 353. doi:10.2307/2307043. JSTOR 2307043.

[19] Friedlander J. and Iwaniec H.(1998), "*The polynomial* $x^2 + y^4$ *captures its primes*", Annals of Mathematics 2 148 , pp 9451040.

[20] Friedlander J. and Iwaniec H. (1996), "*Asymptotic sieve for primes*", A nnals of Mathematics 2 Vol 148, No 3, pp 1041-1065.

[21] Goto, T; Ohno, Y (2008). "*Odd perfect numbers have a prime factor exceeding* 10^8". Mathematics of Computation, Vol. 77 (263): pp. 1859–1868.

[22] Hagis, P. (1980). "*Outline of a Proof that Every Odd Perfect Number has at Least Eight Prime Factors*". Mathematics of Computation, Vol. 35 (151): pp. 1027-1032.

[23] Hagis, P; McDaniel, W. L. (1975). "*On the Largest Prime Divisor of an Odd Perfect Number II*".

[24] Hardy G.H, Wright E.M (2008), "*An introduction to the theory of numbers*", (6th Edition), USA Oxford University press. ISBN 978-0-19-921986-5.

[25] Hardy G. H. and Littlewood J. E. (1922), "*Some problems of 'partitio numerorum*"; III: On the expression of a number as sum of primes, Acta Math. 44, no. 3, 1–70.

[26] Hare, K. G. (2007). "*New techniques for bounds on the total number of prime factors of an OPN*". Math. Comp. 76 no. 260 pp 2241-2248.

[27] Heath-Brown D.R. (2001),"*Primes represented by* x^3+2y^3", Acta Mathematica 186 , 184. pp 1-84

[28] Williamson J. (1782), "*The Elements of Euclid, With Dissertations*", Clarendon Press, Oxford, page 63.

[29] Jenkins, P. M. (2003). "*Odd Perfect Numbers Have a Prime Factor Exceeding* 10^7". Mathematics of Computation, Vol. 72: pp. 1549-1554.

[30] Pinasco J. P. (2009), "*New Proofs of Euclid's and Euler's theorems*", American Mathematical Monthly, volume 116, number 2, pages 172–173.

[31] Whang J. P. (2010), "*Another Proof of the Infinitude of the Prime Numbers*", American Mathematical Monthly, volume 117, number 2, page 181.

[32] Kanold, H. J. (1957). "*Uber Mehrfache Vollkommene Zahlen. II*". J. Reine Agnew. Mathematics, Vol. 197: pp. 82-96.

[33] Kishore, M. (1977). "*Odd Perfect Numbers Not Divisible by* 3 *Are Divisible by at Least Ten Distinct Primes*". Mathematics of Computation, Vol. 31 (137): pp. 274-279.

[34] Kornilowicz A., Rudnicki P. (2004), "*Fundamental theorem of Arithmetic*", Formalized Mathematics 12(2): 179-185.

[35] Laatsch R. (1986), "*Measuring the abundance of integers*", Mathematics Magazine, Mathematical Association of America (MAA) 59 , 84–92.

[36] Linnik Yu. V. (1941), "*The large sieve*", Dokl. Akad. Nauk SSSR 30 , 292294 (Russian).

[37] Loo A. (2011), "*On primes in the interval* $(3n, 4n)$". International Journal of Contemporary Mathematical Sciences 6 (38).

[38] Luca F. and Pomerance C. (2010), "*On the radical of a perfect number*", New York J. Math.16, 23–30.

[39] Montgomery H.L. (1978), "*The analytic principle of the large sieve*", Bull. Amer. Math. Soc. 84 , 547567.

[40] Nielsen, P. P (2006). "*Odd Perfect Numbers Have at Least Nine Distinct Prime Factors*". http://arxiv.org/abs/math.NT/0602485.

[41] Norton, K. K. (1960). "*Remarks on the Number of Factors of an Odd Perfect Number*". Acta Arith, Vol. 6: pp. 365-374.

[42] Ochem, P.; Rao, M. (2012). "*Odd Perfect Numbers are Greater than* 10^{1500}". Mathematics of Computation, Vol. 81 (279): pp. 1869-1877.

[43] Ore O. (1948), "*On the averages of the divisors of a number*", Amer. Math. Monthly, 55, 615–619. MR0027292 (10:284a).

[44] Barkley R. J.; Schoenfeld L., "*Approximate formulas for some functions of prime numbers*", Illinois J. Math 6: 64-94. ISSN 0019-2082.

[45] Ryan R. F. (2003), "*A simpler dense proof regarding the abundancy index*". Mathematics Magazine, Mathematical Association of America (MAA) 76, 299–301.

[46] Selberg A. (1947), "*On an elementary method in the theory of primes.*", Norske Vid. Selsk. Ford., Trondhjem 19, no. 18,64-67.

[47] Shapiro H. N. (1983), "*Introduction to the Theory of Numbers*". Wiley, New York,. MR693458 (84f:10001).

[48] Schinzel A. and Sierpiński W. (1958), "*Sur certaines hypothèses concernant les nombres premiers*", Acta Arith. 4, 185–208.

[49] Steuerwald R. (1937), "*Verschärfung einen notwendigen Bedingung für die Existenz einen ungeraden vollkommenenZ ahl*". S-B Math.-Nat. Abt. Bayer. Akad. Wiss., 68-72.

[50] Touchard, J. (1953). "*On Prime Numbers and Perfect Numbers*". Scripta Math. Vol. 19: pp. 35-39.

[51] Tuckerman, B. (1973). "*A Search Procedure and Lower Bound for Odd Perfect Numbers*". Mathematics of Computation, Vol. 27 (124): pp. 943-949.

[52] McDaniel W. L. (1975), "*On the proof that all even perfect numbers are of Euclids type*", Math. Mag. 48, 107108.

[53] Weiner P. A. (2000), "*The abundancy index, a measure of perfection*". Mathematics Magazine, Mathematical Association of America (MAA) 73, 307–310.

[54] Wissam R. (2013), "*An Introductory Course in Elementary Number Theory.*", Chapters 1,4,7 and 8. http://www.saylor.org/site/wp-content/uploads/2013/05/An-Introductory-in-Elementary-Number-Theory.pdf.

[55] Vardi, I (1991). "*Computational Recreations in Mathematica*". Redwood City, CA: Addison-Wesley, pp. 8 and 224-225,.

[56] Ge Y.(2008), "*Elementary Properties of Cyclotomic Polynomials.*", Chapter 2, www.yimin-ge.com/doc/cyclotomic_polynomials.pdf.