Summer 2015

Expectation Numbers of Cyclic Groups

Miriam Mahannah El-Farrah
Western Kentucky University, mahannah.el-farrah@topper.wku.edu

EXPECTATION NUMBERS OF CYCLIC GROUPS

A Thesis
Presented to
The Faculty of the Department of Mathematics
Western Kentucky University
Bowling Green, Kentucky

In Partial Fulfillment
Of the Requirements for the Degree
Master of Science

By
Miriam Mahannah El-Farrah

August 2015

EXPECTATION NUMBERS OF CYCLIC GROUPS

Date Recommended July 14, 2015

Dominic Lanphier, Director of Thesis

Melanie Autin

Molly Dunkum

Dean, Graduate Studies and Research Date 8-2-15

This thesis is dedicated to my family. Mom and Dad, thank you for always supporting my wild endeavors and always being there when I need you.

Joel, Micah, and Nabeel, you are the three best brothers a girl could ask for. Thanks for always believing in me and encouraging me when I need it.

Rachel, you will never understand how grateful I am for you. Everyday I thank God for bringing you into our lives. Thank you for always supporting me and being an amazing sister(-in-law).

Nathan, Abigail, Lydia, Sophia, thank you for making me the coolest aunt and for always being the shining light in my life.

Everything I am, is because of all of you. I love you very much.

ACKNOWLEDGMENTS

I would like to thank my advisor Dr. Dominic Lanphier for his guidance, knowledge, and assistance; coupled with an abundance of patience and understanding that he has shown throughout this entire process over the past year. I also would like to thank Dr. Molly Dunkum and Dr. Melanie Autin for serving as my committee members. To Dr. Dunkum for always listening and giving advice and guidance and to Dr. Autin for guiding me through the finishing touches of my paper. Finally, thank you to the Department of Mathematics at Western Kentucky University that gave me the opportunity to have an amazing experience. I am grateful to the lessons they have taught me and the wonderful people throughout the department that I have met on this journey.

To my fellow graduate students, this has been an amazingly wild ride. I will never forget all of the fun we have had together over the past two years. A huge thanks to you all for making this a truly memorable experience.

CONTENTS

EXPECTATION NUMBERS OF CYCLIC GROUPS

Miriam Mahannah El-Farrah August 2015 Pages 42

Directed by: Dr. Dominic Lanphier, Dr. Melanie Autin, and Dr. Molly Dunkum

Department of Mathematics Western Kentucky University

When choosing k random elements from a group the k^{th} expectation number is the expected size of the subgroup generated by those specific elements. The main purpose of this thesis is to study the asymptotic properties for the first and second expectation numbers of large cyclic groups.

The first chapter introduces the k^{th} expectation number. This formula allows us to determine the expected size of any group. Explicit examples and computations of the first and second expectation number are given in the second chapter. Here we show example of both cyclic and dihedral groups. In chapter three we discuss arithmetic functions which are crucial to computing the first and second expectation numbers. The fourth chapter is where we introduce and prove asymptotic results for the first expectation number of large cyclic groups. The asymptotic results for the second expectation number of cyclic groups is given in the fifth chapter. Finally, the results are summarized and future work for expectation numbers is discussed.

Chapter 1

Introduction

The question of whether or not a given pair of elements of a group generates that specific group has been well-studied. For example, a classical theorem of Dixon [**6, 7, 8**] asserts that if two elements of the symmetric group S_n are chosen at random, then the likelihood that the two elements generate S_n, or the alternating subgroup A_n, approaches 1 as n goes to infinity. Babai [**3**] and Babai and Hayes [**4**] further studied the probability of two elements generated by the symmetric group. Erdős and Turán in [**9, 10, 11, 12, 13, 14, 15**] developed a statistical group theory and applied it to the study of symmetric groups. A related question is that once elements are chosen, then what is the size of the subgroup generated by those elements?

We are interested in the size of the subgroup generated by a randomly chosen set of k elements of a group G, using a number that we define for the group called the k^{th} expectation number of a group G. The k^{th} expectation number, $E_k(G)$, is the expected size of a subgroup generated by k randomly chosen elements from G using the discrete uniform probability distribution. Thus all elements of G are equally likely to be chosen. Therefore, the k^{th} expectation number measures the average size of the subgroups of G that are generated by k elements. From Lagrange's Theorem, Theorem 7.1 of [**16**], we know that the order $|g|$ of a subgroup must divide the order of the group. If $k > \frac{|G|}{2}$, then the order of the subgroup must be equal to the order of the group G, thus $E_k(G) = |G|$.

We begin with the first expectation number $E_1(G)$, and take $G = C_n$, the cyclic group of order n. We randomly draw one element from the group C_n and then compute

the expected size of the subgroup generated by that single element to determine $E_1(G)$ for the cyclic groups. Note that $E_1(G)$ is simply the average order of the elements of G. Cyclic groups have a simpler and more number-theoretic structure than other groups, which is why we choose to begin here. For cyclic groups, $E_1(C_n)$ was essentially studied in [**20**]. Related results were also obtained in [**18**] and [**19**].

After looking at the first expectation number of C_n, we follow by investigating $E_2(G)$ for cyclic groups. In this part, we will be finding the expectation number that is obtained by choosing at random two elements of the group, instead of just one element.

The k^{th} Expectation Number

Let G be a finite group of order n and set $G = \{g^0 \dots g^{n-1}\}$. For any subset S of G, let $\langle S \rangle$ denote the subgroup of G generated by S. The k^{th} expectation number of G is defined as:

$$E_k(G) = \frac{1}{\binom{n}{k}} \sum_{\{i_1 \dots i_k\} \subseteq \{0 \dots n-1\}} |\langle g^{i_1} \dots g^{i_k} \rangle|,$$

where the $i_1, \dots, i_k$ are distinct. This is the average order of the subgroups generated by k elements of G.

In particular,

$$E_1(G) = \frac{|g^0| + \cdots + |g^{n-1}|}{n}.$$

From Lagrange's Theorem, when $k > \frac{n}{2}$ then $E_k(G) = n$.

We want to start by looking at the expected size, $E_1(G)$, of the subgroup generated by a randomly chosen element of $G = C_n$. The ratio $\frac{E_1(C_n)}{n}$ is the proportion of the

group C_n that we expect a randomly chosen element to generate. For example, we can directly compute that $\frac{E_1(C_{10})}{10} = 0.63$, $\frac{E_1(C_{99})}{99} = 0.6908$, and $\frac{E_1(C_{149})}{149} = 0.9933$. When n is prime, as in the last example, the ratio will be close to 1. For example, in the case of 149, since 149 is prime then 148 of the elements will generate the entire group of C_{149}. Numerical experimentation shows that, on average, the ratio is about 0.7307. More precisely, our first result is the following, where $\zeta(s)$ is the Riemann zeta function.

THEOREM 1.1. $\lim_{x\to\infty} \frac{1}{x} \sum_{1\le n\le x} \frac{E_1(C_n)}{n} = \frac{\zeta(3)}{\zeta(2)} \approx 0.7307.$

Note that, $\zeta(3)$ is Apéry's constant and $\zeta(2) = \frac{\pi^2}{6}$. This result says that if one chooses a random element from a cyclic group C_n with $1 \le n \le x$ and x large, then the element will generate, on average, approximately 73% of the group. A similiar result was obtained in [**17**]. Also see Theorem 10 of [**18**] and [**1**]. Our second result is new and is the following:

THEOREM 1.2. $\lim_{x\to\infty} \frac{1}{x} \sum_{2\le n\le x} \frac{E_2(C_n)}{n} = \frac{\zeta(4)}{\zeta(3)} \approx 0.9004.$

This result says that if one chooses two random elements from a cyclic group C_n with $2 \le n \le x$ and x large, then these two elements will generate, on average, approximately 90% of the group.

Chapter 2

Explicit Examples and Computations

Here we compute some simple examples of expectation numbers for a few basic groups.

The first expectation number for $G = \{g^0, \ldots, g^{n-1}\}$ is

$$E_1(G) = \frac{|g^0| + \cdots + |g^{n-1}|}{n}.$$

For a cyclic group $C_n = \langle a | a^n = 1 \rangle$ we get

$$E_1(C_n) = \frac{1 + |a| + |a^2| + \cdots + |a^{n-1}|}{n}.$$

In particular, for $n = 5$ and $n = 6$ we get,

$$\begin{aligned} E_1(C_5) &= \frac{1 + |a| + |a^2| + |a^3| + |a^4|}{5} \\ &= \frac{1 + 5 + 5 + 5 + 5}{5} \\ &= \frac{21}{5} = 4.2 \end{aligned}$$

and

$$\begin{aligned} E_1(C_6) &= \frac{1 + |a| + |a^2| + |a^3| + |a^4| + |a^5|}{6} \\ &= \frac{1 + 6 + 3 + 2 + 3 + 6}{6} \\ &= \frac{21}{6} = 3.5. \end{aligned}$$

In the same way we get,

$$E_1(C_1) = 1 \qquad E_1(C_2) = 1.5$$

$$E_1(C_3) = 2.33 \qquad E_1(C_4) = 2.75$$

$$E_1(C_5) = 4.2 \qquad E_1(C_6) = 3.5$$

$$E_1(C_7) = 5.14 \qquad E_1(C_8) = 5.375$$

$$E_1(C_9) = 6.778 \qquad E_1(C_{10}) = 6.3.$$

For the second expectation number, we have

$$E_2(G) = \frac{1}{\binom{n}{2}} \sum_{1 \le i < j \le n-1} |\left\langle g^i, g^j \right\rangle|$$

Thus for $C_n = \langle a | a^n = 1 \rangle$,

$$E_2(C_n) = \frac{2}{n(n-1)} \sum_{0 \le i < j \le n-1} |\left\langle a^i, a^j \right\rangle|.$$

For example,

$$\begin{aligned} E_2(C_4) &= \frac{|\langle 1, a \rangle| + |\langle 1, a^2 \rangle| + |\langle 1, a^3 \rangle| + |\langle a, a^2 \rangle| + |\langle a, a^3 \rangle| + |\langle a^2, a^3 \rangle|}{6} \\ &= \frac{4 + 2 + 4 + 4 + 4 + 4}{6} \\ &= \frac{22}{6} = 3.66 \end{aligned}$$

and

$$E_2(C_6) = \frac{\begin{array}{c}|\langle 1,a\rangle| + |\langle 1,a^2\rangle| + |\langle 1,a^3\rangle| + |\langle 1,a^4\rangle| + |\langle 1,a^5\rangle| + |\langle a,a^2\rangle| + |\langle a,a^3\rangle| + |\langle a,a^4\rangle| \\ + |\langle a,a^5\rangle| + |\langle a^2,a^3\rangle| + |\langle a^2,a^4\rangle| + |\langle a^2,a^5\rangle| + |\langle a^3,a^4\rangle| + |\langle a^3,a^5\rangle| + |\langle a^4,a^5\rangle|\end{array}}{15}$$

$$= \frac{6+3+2+3+6+6+6+6+6+6+3+6+6+6+6}{15}$$

$$= \frac{77}{6} = 5.133.$$

Similarly we get

$$E_2(C_1) = 1 \qquad E_2(C_2) = 2$$

$$E_2(C_3) = 3 \qquad E_2(C_4) = 3.66$$

$$E_2(C_5) = 5 \qquad E_2(C_6) = 5.133$$

$$E_2(C_7) = 7 \qquad E_2(C_8) = 7.07$$

$$E_2(C_9) = 8.5 \qquad E_2(C_{10}) = 8.71.$$

For dihedral groups we have,

$$D_n = \left\langle a,b | a^n = b^2 = 1, ab = ba^{n-1} \right\rangle.$$

For example when $n = 3$ and $n = 4$ we have,

$$E_1(D_3) = \frac{1 + |a| + |a^2| + |b| + |ba| + |ba^2|}{6}$$

$$= \frac{1+3+3+2+2+2}{6}$$

$$= \frac{13}{6} = 2.16,$$

$$E_1(D_4) = \frac{1 + |a| + |a^2| + |a^3| + |b| + |ba| + |ba^2| + |ba^3|}{8}$$
$$= \frac{1 + 4 + 2 + 4 + 2 + 2 + 2 + 2}{8}$$
$$= \frac{19}{8} = 2.36.$$

Finally we have

$$E_2(D_3) = \frac{\begin{array}{c} |\langle 1, a\rangle| + |\langle 1, a^2\rangle| + |\langle 1, b\rangle| + |\langle 1, ba\rangle| + |\langle 1, ba^2\rangle| + |\langle a, a^2\rangle| + |\langle a, b\rangle| + |\langle a, ba\rangle| \\ + |\langle a, ba^2\rangle| + |\langle a^2, b\rangle| + |\langle a^2, ba\rangle| + |\langle a^2, ba^2\rangle| + |\langle b, ba\rangle| + |\langle b, ba^2\rangle| + |\langle ba, ba^2\rangle| \end{array}}{15}$$

$$= \frac{3 + 3 + 2 + 2 + 2 + 3 + 6 + 6 + 6 + 6 + 6 + 6 + 6 + 6 + 6}{15}$$
$$= \frac{69}{15} = 4.6.$$

and

$$E_2(D_4) = \frac{\begin{array}{c} |\langle 1, a\rangle| + |\langle 1, a^2\rangle| + |\langle 1, a^3\rangle| + |\langle 1, b\rangle| + |\langle 1, ba\rangle| + |\langle 1, ba^2\rangle| + |\langle 1, ba^3\rangle| + |\langle a, a^2\rangle| \\ + |\langle a, a^3\rangle| + |\langle a, b\rangle| + |\langle a, ba\rangle| + |\langle a, ba^2\rangle| + |\langle a, ba^3\rangle| + |\langle a^2, a^3\rangle| + |\langle a^2, b\rangle| \\ + |\langle a^2, ba\rangle| + |\langle a^2, ba^2\rangle| + |\langle a^2, ba^3\rangle| + |\langle a^3, b\rangle| + |\langle a^3, ba^2\rangle| + |\langle a^3, ba^3\rangle| + |\langle b, ba\rangle| \\ + |\langle b, ba^2\rangle| + |\langle ba, ba^2\rangle| + |\langle ba, ba^3\rangle| + |\langle ba^2, ba^3\rangle| \end{array}}{28}$$

$$E_2(D_4) = \frac{\begin{array}{r}4+2+4+2+2+2+2+4+4+8+8+8+8+4+4+4+4+8+8+8+8\\ +8+8+4+8+8+4+8\end{array}}{28}$$

$$= \frac{154}{28} = 5.5.$$

Note that in the example for $E_2(D_3)$ we computed $ba \cdot ba^2 = b(ab)a^2 = b(ba^2)a^2 = b^2a^4 = a$ so $a \in \langle ba, ba^2 \rangle$. Then $ba^2 \cdot a = ba^3 = b$ so $b \in \langle ba, ba^2 \rangle$. Therefore $\langle ba, ba^2 \rangle = \langle a, b \rangle = D_3$ so $|\langle ba, ba^2 \rangle| = 6$. Other orders of pairs of elements were determined in similar ways.

Chapter 3

Arithmetic Functions and the Möbius Inversion Formula

In this section we introduce the arithmetic functions which are crucial to computing $E_1(C_n)$ and $E_2(C_n)$. We also prove the relevant properties of these functions. These proofs are given in the literature from various sources. Let $f(n)$ be a function from the set of positive integers to the complex numbers, $\mathbb{C}$. We say that $f(n)$ is a multiplicative function and the definition is as follows. Such functions often have deep number-theoretic applications and properties.

Definition 3.1. [**20**] *A function $f(m)$ is said to be multiplicative if $(m, m') = 1$ implies $f(mm') = f(m)f(m')$.*

Lemma 3.2. *If $f(n)$ is multiplicative then $\sum_{d|n} f(d)$ is multiplicative.*

Proof. This proof is Theorem 265 of [**20**]. Let $(m, n) = 1$ and let $m_1, m_2, \ldots, m_k$ be the divisors of m and let $n_1, n_2, \ldots n_l$ be the divisors of n. Then, because $(m_i, n_j) = 1$ for all $1 \leq i \leq k$ and $1 \leq j \leq l$, we have

$$\left(\sum_{d|m} f(d)\right)\left(\sum_{d|n} f(d)\right) = \left(\sum_{i=1}^{k} f(m_i)\right)\left(\sum_{j=1}^{l} f(n_j)\right)$$

$$\sum_{\substack{1\leq i\leq k\\ 1\leq j\leq l}} f(m_i)f(n_j) = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq d}} f(m_i n_j) = \sum_{d|mn} f(d).$$

□

Euler's Totient Function

Euler's totient function, also known as the phi function $\phi(n)$, is an arithmetic function that counts the positive integers less than or equal to n that are relatively prime to n. See Theorem 2.5 on page 51 of [**23**], for example. In other words, if n is a positive integer, then $\phi(n)$ is the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $\gcd(n, k) = 1$. For simplicity, we will denote the greatest common divisor of the integers a, b as (a, b), and also denote the greatest common divisor of an n-tuple of integers $a_1, \ldots, a_n$ by $(a_1, \ldots, a_n)$.

Note that if n is a prime then $\phi(n) = n - 1$, since a prime has no factor greater than 1 other than itself. Euler's formula for $\phi(n)$ is given by the following,

THEOREM 3.3 (Theorem 2.19 [**23**]).

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

PROOF. For a positive integer n and a prime p dividing n, there are $\frac{n}{p}$ positive integers less than or equal to n with p as a factor. There are $n - \frac{n}{p}$ positive integers less than or equal to n without p as a factor. First we consider the term $n - \sum_{p|n} \frac{n}{p}$. For two distinct primes p, q that divide n, the term $\sum_{p|n} \frac{n}{p}$ counts twice those positive integers less than or equal to n that have both p and q as a factor. By the Inclusion-Exclusion principle, we have to add those terms. We consider,

$$n - \sum_{p|n} \frac{n}{p} + \sum_{p,q|n} \frac{n}{pq}.$$

Continuing, we get that for $p, q, r, \ldots$ primes that divide n,

$$n - \sum_{p|n} \frac{n}{p} + \sum_{p,q|n} \frac{n}{pq} - \sum_{p,q,r|n} \frac{n}{pqr} + \ldots$$

is the number of positive integers less than or equal to n that are relatively prime to n. Thus we have,

$$\phi(n) = n - \sum_{p|n} \frac{n}{p} + \sum_{p,q|n} \frac{n}{pq} - \sum_{p,q,r|n} \frac{n}{pqr} + \ldots$$

$$= n\left(1 - \sum_{p|n} \frac{1}{p} + \sum_{p,q|n} \frac{1}{pq} - \ldots\right).$$

Note that a direct computation shows that

$$\prod_{p|n}\left(1 - \frac{1}{p}\right) = 1 - \sum_{p|n} \frac{1}{p} + \sum_{p,q|n} \frac{1}{pq} - \sum_{p,q,r|n} \frac{1}{pqr} + \ldots,$$

and we get

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

□

For example, let $n = 10$. The prime divisors of 10 are 2 and 5. Using Euler's formula, we have $10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4$. This tells us that there are four integers between 1 and 10 that are relatively prime to 10. If we consider all of the primes that are relatively prime up to 10 we have $1, 3, 7, 9$. Since 10 is a product of two primes, 2 and 5, we see that $\phi(5) = 4$ and $\phi(2) = 1$ so, $\phi(5)\phi(2) = 4 = \phi(10)$. More generally, Theorem 3.6 will show that the totient function, $\phi(n)$, is a multiplicative function, which means

if two numbers m and n are relatively prime to one another then $\phi(mn) = \phi(m)\phi(n)$. See Theorem 2.15 of [**23**].

Jordan's Totient Function

Jordan's totient function generalizes Euler's totient function. Let k be a positive integer, then Jordan's totient function $J_k(n)$ of a positive integer n is the number of k-tuples of positive integers all less than or equal to n that are relatively prime to n [**22**]. In other words, the number of positive integers (non-ordered and not necessarily distinct) $1 \leq a_1, \ldots, a_k \leq n$ so that $((a_1, \ldots, a_k), n) = 1$. The formula for $J_k(n)$ that is analogous to Euler's formula is

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right).$$

The proof is similar to the proof of Euler's formula for $\phi(n)$ from Theorem 3.3. Note that $J_1(n) = \phi(n)$.

Divisor Function

The sum of positive divisors function, $\sigma_k(n)$, for a real or complex number k is defined as the sum of the k^{th} powers of the positive divisors of n [**20**]. It can be written as

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

For $n = p_1^{k_1} \ldots p_r^{k_r}$ with p_j all distinct primes, we have an explicit formula for $\sigma_k(n^m)$; see Theorem 275 on page 311 of [**20**].

LEMMA 3.4. *If $n = p_1^{k_1} \ldots p_r^{k_r}$ with p_j distinct primes, then*

$$\sigma_k(n^m) = \prod_{j=1}^{r} \frac{p_j^{(k_j m+1)k} - 1}{p_j^k - 1}.$$

PROOF. Note that n^k is multiplicative, so by Lemma 3.2 we see that $\sigma_k(n)$ is also multiplicative. As $n = p_1^{k_1} \dots p_r^{k_r}$ and

$$\begin{aligned}
\sigma_k(p_j^{k_j m}) &= \sum_{d \mid p_j^{k_j m}} d^k \\
&= 1^k + p_j^k + \left(p_j^2\right)^k + \cdots + \left(p_j^{k_j m}\right)^k \\
&= 1^k + \left(p_j^k\right)^1 + \left(p_j^k\right)^2 + \cdots + \left(p_j^k\right)^{k_j m} \\
&= \frac{1 - \left(p_j^k\right)^{k_j m+1}}{1 - p_j^k} = \frac{p_j^{(k_j m+1)k} - 1}{p_j^k - 1},
\end{aligned}$$

then we see that

$$\sigma_k(n^m) = \prod_{j=1}^{r} \sigma_k\left(p_j^{k_j m}\right) = \prod_{j=1}^{r} \frac{p_j^{(k_j m+1)^k} - 1}{p_j^k - 1}.$$

□

The Riemann Zeta Function

The Riemann zeta function $\zeta(s)$ is a function of a complex variable s. The following infinite series converges for all complex numbers s with real part greater than 1, and is the definition of $\zeta(s)$ [**20**]:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \dots$$

A different expression for $\zeta(s)$ is

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx,$$

where $\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt$ is the gamma function. This formula can be modified to give an expression for $\zeta(s)$ that is valid for all $s \in \mathbb{C}$, with $s \neq 1$. Therefore $\zeta(s)$ can be defined for any $s \in \mathbb{C}$ with $s \neq 1$.

For $n \in \mathbb{Z}_{\geq 1}$, Euler found the values of $\zeta(s)$ at even positive integers. This formula is

$$\zeta(2n) = (-1)^{n+1} \frac{B_{2n} (2\pi)^{2n}}{2(2n)!},$$

where B_{2n} are the Bernoulli numbers [**20**]. The Bernoulli numbers are rational numbers so that

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

An explicit expression for the Bernoulli numbers is [**20**]

$$B_n = \sum_{j=0}^{m} \sum_{k=0}^{j} (-1)^k \binom{j}{k} \frac{k^n}{j+1}.$$

As examples, Euler showed that

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6},$$

and

$$\zeta(4) = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots = \frac{\pi^4}{90}.$$

The values of $\zeta(s)$ at the odd positive integers are still largely mysterious, but some interesting results have been found. Apéry showed that $\zeta(3)$ is irrational [**2**]. Later Ball and Rivoal showed that an infinite number of $\zeta(2k+1)$'s are irrational [**5**] and similarly

in [**25**], but they did not give further precise examples. However, Rivoal did show that at least one of $\zeta(5), \zeta(7), \zeta(9)$, or $\zeta(11)$ is irrational [**24**].

The Möbius Function

The Möbius function $\mu(n)$ is defined on positive integers n as follows [**20**]:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } a^2 | n \text{ for some integer } a > 1 \\ (-1)^r, & \text{if } n = p_1 p_2 \dots p_r, \ p_i \text{ distinct primes.} \end{cases}$$

This implies that the Möbius function will be zero if and only if n has a square factor larger than one. An important application of the Möbius function is in obtaining a different formula for Euler's Totient function. Note that $\mu(n)$ is a multiplicative function. The following result will be used to establish the Möbius Inversion Formula, it can be found in [**20**].

Lemma 3.5.

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

Proof. Note that if $(m, n) = 1$ then $\mu(m, n) = \mu(m)\mu(n)$. Thus $\mu(m)$ is multiplicative, so by Lemma 3.2, $\sum_{d|n} \mu(d)$ is also multiplicative. Set $h(m) = \sum_{d|n} \mu(d)$. Since $h(m)$ is multiplicative, we just need to show that $h(p^k) = 0$ for $k \geq 1$.

We have,

$$\begin{aligned} h(p^k) = \sum_{d|p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) + 0 + \cdots + 0 \end{aligned}$$

$$= 1 + (-1) = 0.$$

For $m = p_1^{k_1} \dots p_r^{k_r}, p_j$ distinct primes and $k_j \geq 1$,

$$h(m) = h(p_1^{k_1}) \dots h(p_r^{k_r}) = 0 \dots 0 = 0.$$

Since $h(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$, we have the result. □

Möbius Inversion Formula

One of the most useful tools for studying arithmetic functions is the Möbius Inversion Formula.

THEOREM 3.6 (Möbius Inversion Formula. Theorem 266 of [**20**]).

If $f(n)$ and $g(n)$ are multiplicative functions of the integers, so that

$$g(n) = \sum_{d|n} f(d), \text{ for every } n \in \mathbb{Z},$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right), \text{ for every } n \in \mathbb{Z}.$$

PROOF. By the definition of $g(n)$ we have $g\left(\frac{n}{d}\right) = \sum_{c|\frac{n}{d}} f(c)$. Therefore,

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

$$= \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d)$$

By Lemma 3.5, the only c that divides n so that $\sum_{d|\frac{n}{c}} \mu(d)$ is not 0 is $c = n$. Thus we have $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = f(n) \sum_{d|\frac{n}{n}} \mu(d) = f(n)$. □

Big O Notation

Big O notation describes the limiting behavior of a function when the variable tends towards a particular value or infinity. This notation is useful for determining the size of the error term in a limit. We will use it in further research to study our main results more closely.

Let f and g be two functions defined on some subset of the real numbers. Then,

$$f(x) = O(g(x)) \text{ as } x \to \infty$$

if and only if there is a positive constant M such that for all sufficiently large values of x, the absolute value of $f(x)$ is at most M multiplied by the absolute value of $g(x)$ [**23**]. That is, $f(x) = O(g(x))$ if and only if there exists a positive real number M and a real number x_0 such that

$$|f(x)| \leq M|g(x)| \text{ for all } x \geq x_0.$$

Chapter 4

Expected Size of a Subgroup; The First Expectation Number

To study $E_1(C_n)$, we first obtain an explicit formula for $E_1(C_n)$. Recall that

$$E_1(C_n) = \frac{1}{n} \sum_{0 \le i \le n-1} |a^i|.$$

The first important formula that we obtain expresses the first expectation number in terms of arithmetic functions from Chapter 3. Then we can use number-theoretic arguments to prove the main result about $E_1(C_n)$. We first establish some (well-known) properties about cyclic groups.

Proposition 4.1 (Theorem 0.2 [**16**]).

For $a, b \in \mathbb{Z}_{>0}$ there exists $x, y \in \mathbb{Z}$ so that $(a, b) = ax + by$.

Proof. Let $S_{ab} = \{ax + by | x, y \in \mathbb{Z}, ax + by > 0\}$. Note that $S_{ab} \neq \varnothing$ because if $ax + by < 0$ we can take $a(-x) + b(-y) > 0$. The well ordering principle states that given any nonempty set of positive integers there must be a smallest element in the set. Thus there must be some smallest element in S_{ab}, say $d = ax + by$.

By the division algorithm, there exists a unique set of integers q, r with $q > 0$ so that $a = dq + r$ and $0 \le r < d$. Now, if $r > 0$ then $r = a - dq = a - (ax + by)q = a - aqx - byq = a(1 - qx) + b(-yq)$. This must be in S_{ab}, but $r < d$. This contradicts the fact that d must be the smallest element in S_{ab}, so we must have $r = 0$. Thus $a = dq$ so $d|a$. The same argument works with b, so $b = dq' + r'$ with $0 \le r' < d$ implies $r' = 0$, and this gives $d|b$. Therefore d is a divisor of a and b. Now suppose that D is a divisor of a and b so

$a = Dn, b = Dm$. Then $d = ax + by = Dnx + Dmy = D(nx + my)$ so D must also be a divisor of d. It follows that d must be the greatest common divisor of a and b. □

We use this result to prove a fact which we needed about cyclic groups.

LEMMA 4.2. *Let* $C_n = \langle a | a^n = 1 \rangle$ *for* $k \in \mathbb{Z}_{\geq 1}$. *Then* $\langle a^k \rangle = \langle a^{(n,k)} \rangle$ *and* $|a^k| = \dfrac{n}{(n,k)}$.

PROOF. This is Theorem 4.2 of [**20**].

Since $(n,k)|k$ then $a^k = a^{(n,k)\cdot l} = \left(a^{(n,k)}\right)^l$ for some $l \in \mathbb{Z}_{\geq 1}$. Thus $a^k \in \langle a^{(n,k)} \rangle$ and so $\langle a^k \rangle \leq \langle a^{(n,k)} \rangle$. By Proposition 4.1, $(n,k) = nx + ky$ for some $x, y \in \mathbb{Z}$. Thus, $a^{(n,k)} = a^{nx+ky} = (a^n)^x (a^k)^y = 1^x (a^k)^y = (a^k)^y \in \langle a^k \rangle$. Thus, $\langle a^{(n,k)} \rangle \leq \langle a^k \rangle$ and so $\langle a^k \rangle = \langle a^{(n,k)} \rangle$.

If $d|n$, then the order of a^d is $\dfrac{n}{d}$. As $|a^k| = |a^{(n,k)}|$ and $(n,k)|n$, then the order of $a^{(n,k)} = \dfrac{n}{(n,k)}$. So the order of a^k is also $\dfrac{n}{(n,k)}$. □

The first main result of this chapter is the following expression of the first expectation number, $E_1(C_n)$, in terms of arithmetic functions.

PROPOSITION 4.3. $E_1(C_n) = \dfrac{1}{n} \displaystyle\sum_{d|n} d\phi(d)$.

PROOF. By LaGrange's Theorem, any element in C_n must have order which is a divisor of n. Therefore any element of C_n has order d with $d|n$. Thus,

$$E_1(C_n) = \frac{|a_1| + \cdots + |a_n|}{n} = \frac{1}{n} \sum_{d|n} d \times (\text{the number of elements of } C_n \text{ of order } d).$$

We now determine the number of elements of C_n that have order d, for d a divisor of n. Suppose $a^k \in C_n$ has order d for $d|n$. Then by Lemma 4.2, $\dfrac{n}{(n,k)} = |a^k| = d$ so

$(n,k) = \frac{n}{d}$. Then by Lemma 4.2, $\left\langle a^k \right\rangle = \left\langle a^{(n,k)} \right\rangle = \left\langle a^{\frac{n}{d}} \right\rangle$. Let $(j,d) = 1$. Then $\left(a^{\frac{nj}{d}}\right)^d = a^{nj} = 1$ and so the order of $a^{\frac{nj}{d}}$ is at most d. However, since $(j,d) = 1$, the order cannot be strictly smaller than d because then there would be some prime $p|n$ which divides the denominator of $\frac{jk}{d}$. Then for any $x \in \mathbb{Z}_{>0}, \frac{njx}{d}$ is not a multiple of n, and so $a^{\frac{njx}{d}} \neq 1$. Thus $(j,d) = 1$ if and only if $a^{\frac{nj}{d}}$ has order d. Therefore there are $\phi(d)$ elements in C_n of order d. Thus we get

$$E_1(C_n) = \frac{1}{n} \sum_{d|n} d\phi(d).$$

□

A consequence of this result is the following. From the discussion about $\phi(n)$ we know that $\phi(n)$ is multiplicative. That is, if $(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$. Thus $n\phi(n)$ is also multiplicative. From Lemma 3.2, $\sum_{d|n} d\phi(d)$ is multiplicative, and so we have that $E_1(C_n)$ is multiplicative. This result and the previous expression for $E_1(C_n)$ allow us to get another expression for $E_1(C_n)$ in terms of sums of divisor functions. This result is in [**18**]. Note that $E_1(C_n)$ is sequence $A057660$ in the online integer sequences database [**26**].

PROPOSITION 4.4. $E_1(C_n) = \frac{\sigma_2(n^2)}{n\sigma_1(n^2)}$.

PROOF. In $C_n = \left\langle a | a^{p^k} = 1 \right\rangle$, every element is of the form a^l with $0 \leq l < p^k$. Then l is divisible by an exact power of p, say p^j with $0 \leq j < k$. Thus, $l = p^j m$ where p does not divide $m, 0 \leq j < k$, and $1 \leq m \leq p^{k-j}$. Therefore every element in C_{p^k} can be written in the form $a^{p^j m}$ where $0 \leq j < k, 0 \leq m \leq p^{k-j}$, and $(m, p^{k-j}) = 1$.

Since $\left(a^{p^j m}\right)^{p^{k-j}} = a^{p^k m} = \left(a^{(p^k)}\right)^m = 1^m = 1$, we see that $a^{p^j m}$ generates a subgroup of C_{p^n} of order p^{k-j}.

Now, for a fixed j, the number of elements in C_{p^k} of the form $a^{p^j m}$ with $1 \le m \le p^{k-j}$ and $\left(m, p^{k-j}\right) = 1$ is $\phi(p^{k-j})$. Thus there are precisely $\phi(p^{k-j})$ elements in C_{p^k} that generate a subgroup of size p^{k-j} for $0 \le j < k$. Thus, the expected size of a subgroup in C_{p^k} is

$$E_1(C_{p^k}) = \frac{1}{p^k}\left(1 + \sum_{j=0}^{k-1} p^{k-j}\phi(p^{k-j})\right) = \frac{1}{p^k}\left(1 + \sum_{j=1}^{k} p^j \phi(p^j)\right)$$

$$= \frac{1}{p^k}\left(1 + \sum_{j=1}^{k} p^j (p^j - p^{j-1})\right)$$

$$= \frac{p^{2k+1}+1}{p^k(p+1)}.$$

For $n = p_1^{k_1} \dots p_r^{k_r}$ we have, by the multiplicativity of $E_1(C_n)$,

$$E_1(C_n) = E_1(C_{p_1{}^{k_1}}) \dots E_1(C_{p_r{}^{k_r}}) = \frac{p_1^{2k_1+1}+1}{p_1^{k_1}(p_1+1)} \dots \frac{p_r^{2k_r+1}+1}{p_r^{k_r}(p_r+1)}$$

$$= \frac{1}{p_1^{k_1} \dots p_r^{k_r}} \prod_{j=1}^{r} \frac{p_j^{2k_j+1}+1}{p_j+1} = \frac{1}{n} \prod_{j=1}^{r} \frac{p_j^{2k_j+1}+1}{p_j+1} \cdot \frac{p_j^{2k_j-1}+1}{p_j^{2k_j+1}-1} \cdot \frac{p_j-1}{p_j-1}$$

$$= \frac{1}{n} \prod_{j=1}^{r} \frac{p_j-1}{p_j^{2k_j+1}-1} \prod_{j=1}^{r} \frac{p_j^{(2k_j+1)2}-1}{p_j^2-1} = \frac{1}{n} \cdot \frac{1}{\sigma_1(n^2)} \cdot \sigma_2(n^2),$$

where we used the product expansion of $\sigma_k(m)$ as given in Lemma 3.4 and as found in Theorem 274 of [**20**]. □

Note that the Möbius Inversion Formula applied to Proposition 4.3 gives the expression $\phi(n) = \sum_{d|n} \frac{\mu(d)}{d} E_1(C_{\frac{n}{d}})$. As another application of this formula for $E_1(C_n)$, we can get a generating function for $E_1(C_n)$ as follows.

PROPOSITION 4.5. $\sum_{n=1}^{\infty} \frac{E_1(C_n)}{n^s} = \frac{\zeta(s-1)\zeta(s+1)}{\zeta(s)}$ *for* $Re(s) > 2$, *where* $Re(s)$ *is the real part of a complex number* s.

PROOF. There is a direct proof that uses standard methods, but to be concise we give the following. We have $\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$ from Theorem 288 of [**20**]. Therefore,

$$\frac{\zeta(s-1)\zeta(s+1)}{\zeta(s)} = \left(\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{n^{-1}}{n^s}\right)$$

$$= \sum_{n=1}^{\infty} \frac{\sum_{d|n} \phi(d) \left(\frac{n}{d}\right)^{-1}}{n^s} = \sum_{n=1}^{\infty} \frac{E_1(C_n)}{n^s}.$$

□

As an application of this result we obtain another formula involving $E_1(C_n)$. The coefficients of $\zeta(s) = \sum_{n=1}^{\infty} E_1(C_n) n^{-s}$ are

$$\left(\sum_{m=1}^{\infty} m^{-s}\right)\left(\sum_{n=1}^{\infty} E_1(C_n) n^{-s}\right) = \sum_{m,n=1}^{\infty} m^{-s} E_1(C_n) n^{-s}$$

$$= \sum_{m,n=1}^{\infty} E_1(C_n)(mn)^{-s}$$

Change variables to let $mn = N$, and then n is a divisor of N. This summation is

$$\sum_{m,n=1}^{\infty} E_1(C_n)(mn)^{-s} = \sum_{N=1}^{\infty} \sum_{d|n} E_1(C_d) N^{-s}.$$

Similarly,

$$\zeta(s-1)\zeta(s+1) = \sum_{m=1}^{\infty} m^{-s+1} \sum_{n=1}^{\infty} n^{-s-1}$$
$$= \sum_{m,n=1}^{\infty} \frac{m}{n}(mn)^{-s}.$$

Set $mn = N$ and then n is a divisor of N, and $m = \dfrac{N}{n}$.

Now this summation is

$$\sum_{m,n=1}^{\infty} \frac{m}{n}(ms)^{-s} = \sum_{N=1}^{\infty} \sum_{d|N} \frac{\frac{N}{d}}{d} \cdot N^{-s}$$
$$= \sum_{N=1}^{\infty} N \sum_{d|N} \frac{1}{d^2} N^{-s}.$$

Thus, comparing coefficients we get

$$\sum_{d|N} E_1(C_d) = N \sum_{d|N} \frac{1}{d^2}.$$

Proof of Theorem 1.1

We now use the previous expression, Proposition 4.3, for $E_1(C_n)$ in terms of $\phi(n)$ to prove Theorem 1.1. We first establish some preliminary results. Note that we can take a subsequence $\{x\}$ going to infinity because the limits of Theorem 1.1 and Theorem 1.2 are increasing. We can assume x has the appropriate divisibility properties such as $x|b$, etc.

LEMMA 4.6. $\sum_{d|n} \phi(d) = n.$

PROOF. This proof is Theorem 63 of [**20**]. Since $\phi(n)$ is multiplicative, $\sum_{d|n} \phi(d)$ is multiplicative. This is given in Theorem 4.4 on page 190 of [**23**]. Thus for $n = p_1^{l_1} \dots p_k^{l_k}$ we have

$$\sum_{d|n} \phi(d) = \left(\sum_{d|p_1^{l_1}} \phi(d) \right) \dots \left(\sum_{d|p_n^{l_n}} \phi(d) \right).$$

Further,

$$\sum_{d|p^l} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^l)$$

$$= 1 + p - 1 + p^2 - p + \dots + p^l - p^{l-1} = p^l,$$

so

$$\sum_{d|n} \phi(d) = p_1^{l_1} \dots p_k^{l_k} = n.$$

□

The Möbius Inversion Formula (Theorem 3.6) applied to the expression $\sum_{d|n} \phi(d) = n$, gives the following formula for Euler's totient function. This is Theorem 1.36 of [**21**]:

THEOREM 4.7. $\phi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}$.

LEMMA 4.8. $\sum_{n \le x} \frac{\phi(n)}{n} = x \sum_{1 \le d \le x} \frac{\mu(d)}{d^2}$.

PROOF. We have $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$ from Theorem 4.7. Therefore,

$$\sum_{n=1}^{x} \frac{\phi(n)}{n} = \sum_{n \le x} \frac{1}{n} \cdot n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{n \le x} \sum_{d|n} \frac{\mu(d)}{d}$$

$$\sum_{\substack{d,d' \in \mathbb{Z}_{>0} \\ 1 \le dd' \le x}} \frac{\mu(d)}{d} = \sum_{d=1} \frac{\mu(d)}{d} \sum_{d'=1}^{\frac{x}{d}} 1$$

$$= \sum_{d=1}^{x} \frac{\mu(d)}{d} \cdot \frac{x}{d} = x \sum_{d=1}^{x} \frac{\mu(d)}{d^2}.$$

□

The following proof is essentially a sketch, and the details can be found in [**20**].

THEOREM 4.9 (Theorem 287 [**20**]). *For* $Re(s) > 1$,

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

PROOF. From the definition of the function μ,

$$1 - p^{-s} = 1 + \mu(p)p^{-s} + \mu(p^2)p^{-2s} + \mu(p^3)p^{-3s} + \dots,$$

and since both products below are convergent for $Re(s) > 1$, we have

$$\prod_{p \text{ prime}} (1 - p^{-s}) = \prod_{p \text{ prime}} (1 + \mu(p)p^{-s} + \mu(p^2)p^{-2s} + \mu(p^3)p^{-3s} + \dots).$$

Then we have

$$\frac{1}{\zeta(s)} = \prod_{p \text{ prime}} (1 - p^{-s})$$

and

$$\prod_{p \text{ prime}} \left(1 + \mu(p)p^{-s} + \mu(p^2)p^{-2s} + \dots\right) = \sum_{n-1}^{\infty} \mu(n)n^{-s}.$$

Putting these two equations together gives the result. □

Since $E_1(C_n) = \frac{1}{n}\sum_{d|n}\phi(d)d$ from Proposition 4.3, following arguments given in Hardy-Wright [**20**] we have

$$\sum_{1\le n\le x}\frac{E_1(C_n)}{n} = \sum_{1\le n\le x}\frac{1}{n^2}\cdot\sum_{d|n}\phi(d)d = \sum_{1\le ab\le x}\frac{1}{(ab)^2}\phi(a)a = \sum_{1\le b\le x}\frac{1}{b^2}\sum_{1\le a\le\frac{x}{b}}\frac{\phi(a)}{a},$$

where a and b are positive integers, such that $ab = n$.

Thus we have,

$$\sum_{1\le n\le x}\frac{E_1(C_n)}{n} = \sum_{1\le b\le x}\frac{1}{b^2}\sum_{1\le a\le\frac{x}{b}}\frac{\phi(a)}{a}$$

$$= \sum_{1\le b\le x}\frac{1}{b^2}\cdot\frac{x}{b}\sum_{1\le d\le\frac{x}{b}}\frac{\mu(d)}{d^2}$$

$$= x\sum_{1\le b\le x}\frac{1}{b^3}\sum_{1\le d\le\frac{x}{b}}\frac{\mu(d)}{d^2}.$$

Taking limits we get,

$$\lim_{x\to\infty}\frac{1}{x}\sum_{1\le n\le x}\frac{E_1(C_n)}{n} = \lim_{x\to\infty}\frac{1}{x}\cdot x\sum_{1\le b\le x}\frac{1}{b^3}\sum_{1\le d\le\frac{x}{b}}\frac{\mu(d)}{d^2}$$

$$= \sum_{b=1}^{\infty}\frac{1}{b^3}\cdot\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}.$$

We have $\sum_{b=1}^{\infty}\frac{1}{b^3} = \zeta(3)$ from the definition of the Riemann Zeta function. We also have $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}$ from Theorem 4.9. Thus,

$$\lim_{x\to\infty}\frac{1}{x}\sum_{1\le n\le x}\frac{E_1(C_n)}{n} = \sum_{b=1}^{\infty}\frac{1}{b^3}\cdot\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \zeta(3)\frac{1}{\zeta(2)}.$$

This completes the proof of Theorem 1.1.

Chapter 5

The Second Expectation Number

In this Chapter we prove Theorem 1.2. We follow a similar method as in Chapter 4. We study the second expectation number of cyclic groups,

$$E_2(C_n) = \frac{1}{\binom{n}{2}} \sum_{0 \le i < j \le n-1} |\left\langle a^i, a^j \right\rangle|$$

We first show some similar results as done in Chapter 4 about cyclic groups C_n.

Lemma 5.1. *Let* $C_n = \langle a | a^n = 1 \rangle$. *Then* $\left\langle a^i, a^j \right\rangle = \left\langle a^{(i,j)} \right\rangle$.

Proof. Note that every element of $\langle a^i, a^j \rangle$ is of the form $(a^i)^x (a^j)^y$ for some $x, y \in \mathbb{Z}_{\ge 0}$. Further, for any $x, y \in \mathbb{Z}_{\ge 0}, (a^i)^x (a^j)^y \in \langle a^i, a^j \rangle$. As $(a^i)^x (a^j)^y = a^{ix+jy}$ and there exists $x, y \in \mathbb{Z}_{\ge 0}$ so that $ix + jy = (i, j)$ then $a^{(i,j)} = a^{ix+jy} = (a^i)^x (a^j)^y \in \langle a^i, a^j \rangle$. Thus

$$a^{(i,j)} \in \left\langle a^i, a^j \right\rangle,$$

and,

$$\left\langle a^{(i,j)} \right\rangle \subseteq \left\langle a^i, a^j \right\rangle.$$

Since $(i, j) | i$ and $(i, j) | j$, then

$$a^i, a^j \in \left\langle a^{(i,j)} \right\rangle,$$

and therefore

$$\left\langle a^i, a^j \right\rangle \subseteq \left\langle a^{(i,j)} \right\rangle,$$

and this gives the result. □

We want to count the number of non-ordered possibly equal pairs (i,j) with $1 \leq i,j \leq n$ so that $((i,j),n) = 1$.

LEMMA 5.2. *For $C_n = \langle a | a^n = 1 \rangle$ we have $\langle a^i, a^j \rangle = \langle a^{(i,j)} \rangle = \langle a^{((i,j),n)} \rangle$.*

PROOF. From Lemma 5.1 we have $\langle a^i, a^j \rangle = \langle a^{(i,j)} \rangle$. Now, from Lemma 4.2, $\langle a^k \rangle = \langle a^{(k,n)} \rangle$. Thus $\langle a^{(i,j)} \rangle = \langle a^{((i,j),n)} \rangle$, and this gives the result. □

The first goal is to express $E_2(C_n)$ using arithmetic functions, just as we expressed $E_1(C_n)$ in terms of arithmetic functions in Chapter 4. However, the expression obtained for $E_2(C_n)$ will be a bit more complicated.

LEMMA 5.3. *The number of ordered pairs (i,j) with $i < j$ so that $((i,j),n) = 1$ is* $\dfrac{J_2(n) - \phi(n)}{2}$.

PROOF. Recall that $J_2(n)$ is the number of non-ordered and not necessarily distinct pairs of integers (i,j) with $1 \leq i,j \leq n$ with $((i,j),n)) = 1$. Now, $\phi(n)$ is the number of $i's$ so that $1 \leq i \leq n$ and $(n,i) = 1$. Thus, $\phi(n)$ also gives the number of pairs (i,i) with $1 \leq i \leq n$ so that $((i,i),n) = 1$.

Thus, $J_2(n) - \phi(n)$ is the number of non-ordered pairs (i,j) with $1 \leq i,j \leq n$, and $i \neq j$ such that $((i,j),n) = 1$. To get the number of ordered pairs we simply divide by 2. Thus $\dfrac{J_2(n) - \phi(n)}{2}$ is the number of such pairs (i,j) with $1 \leq i,j \leq n$ and $i < j$ so that $((i,j),n) = 1$. □

From Lemma 5.1, $\langle a^i, a^j \rangle = \langle a^{((i,j),n)} \rangle$. Thus from Lemma 4.2 we have

$$\left| \langle a^i, a^j \rangle \right|$$

$$= \left|\left\langle a^{((i,j),n)} \right\rangle\right|$$

$$= \left|a^{((i,j),n)}\right|$$

$$= \frac{n}{((i,j),n)}.$$

Therefore,

$$\sum_{0\le i<j\le n-1} |\left\langle a^i, a^j \right\rangle| = \sum_{0\le i<j\le n-1} \frac{n}{((i,j),n)}$$

$$= \sum_{d|n} \frac{n}{d} \times (\text{the number of ordered pairs } (i,j) \text{ with } i<j \text{ so that } ((i,j),n) = d).$$

By Lemma 5.3 this is

$$\sum_{d|n} \left(\frac{n}{d}\right) \left(\frac{J_2\left(\frac{n}{d}\right) - \phi\left(\frac{n}{d}\right)}{2}\right) = \frac{1}{2} \sum_{d|n} dJ_2(d) - d\phi(d)$$

Hence we have an expression for $E_2(C_n)$ in terms of arithmetic functions, analogous to a similar expression for $E_1(C_n)$ given in the previous chapter.

Proof of Theorem 1.2

Using this expression for $E_2(C_n)$,

PROPOSITION 5.4. $E_2(C_n) = \dfrac{1}{n(n-1)} \displaystyle\sum_{d|n} dJ_2(d) - d\phi(d),$

we get

$$\frac{1}{x} \sum_{1<n\le x} \frac{E_2(C_n)}{n} = \frac{1}{x} \sum_{1<n\le x} \frac{1}{n} \frac{1}{\frac{n(n-1)}{2}} \left(\frac{1}{2} \sum_{d|n} dJ_2(d) - \frac{1}{2} \sum_{d|n} d\phi(d)\right)$$

$$= \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \left(\sum_{d|n} dJ_2(d) - \sum_{d|n} d\phi(d)\right)$$

$$= \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} dJ_2(d) - \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d).$$

Note that simple algebra gives us, for $n > 1$,

$$\frac{1}{n^2(n-1)} = \frac{1}{n^3} + \frac{1}{n^3(n-1)};$$

thus we have

$$\frac{1}{x} \sum_{1<n\le x} \frac{E_2(C_n)}{n} = \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} dJ_2(d) - \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d)$$

$$= \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3} \sum_{d|n} dJ_2(d) + \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d) - \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d).$$

We consider the three terms

$$\frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3} \sum_{d|n} dJ_2(d),$$

$$\frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d),$$

and

$$\frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d)$$

separately.

We first get a description of $J_k(n)$ in terms of other arithmetic functions.

LEMMA 5.5. $\sum_{d|n} J_k(d) = n^k$.

PROOF. From the formula $J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right)$ we see that $J_k(n)$ is multiplicative. Therefore, by Lemma 3.2, $\sum_{d|n} J_k(d)$ is also multiplicative. For $n = p_1^{l_1} \dots p_r^{l_r}$, with the p_j distinct primes, we have

$$\sum_{d|n} J_k(d) = \left(\sum_{d|p_1^{l_1}} J_k(d)\right) \dots \left(\sum_{d|p_r^{l_r}} J_k(d)\right).$$

Further,

$$J_k(p^j) = \left(p^j\right)^k \prod_{p|p^j} \left(1 - \frac{1}{p^k}\right) = p^{jk}\left(1 - \frac{1}{p^k}\right) = p^{jk} - p^{(j-1)k}$$

Thus,

$$\begin{aligned}\sum_{d|p^l} J_k(d) &= J_k(1) + J_k(p) + J_k(p^2) + \dots + J_k(p^l) \\ &= 1 + (p^n - 1) + (p^{2k} - p^2) + \dots + (p^{lk} - p^{(l-1)k} \\ &= p^{lk}.\end{aligned}$$

We have,

$$\sum_{d|n} J_k(d) = \left(\sum_{d|p_1^{l_1}} J_k(d)\right) \dots \left(\sum_{d|p_r^{l_r}} J_k(d)\right)$$
$$p^{l_1 k} \dots p^{l_r k}$$
$$\left(p_1^{l_1} \dots p_r^{l_r}\right)^k = n^k.$$

□

Since $\sum_{d|n} J_k(d) = n^k$, then by the Möbius Inversion Formula (Theorem 3.6) we have

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

We now determine the limits of the three terms that appear in the expression for

$$\frac{1}{x}\sum_{1<n\leq x}\frac{E_2(C_n)}{n}.$$

LEMMA 5.6. $\lim_{x\to\infty}\frac{1}{x}\sum_{1<n\leq x}\frac{1}{n^3}\sum_{d|n}dJ_2(d)=\frac{\zeta(4)}{\zeta(3)}$.

PROOF.

$$\frac{1}{x}\sum_{1<n\leq x}\frac{1}{n^3}\sum_{d|n}dJ_2(d)=\frac{1}{x}\sum_{\substack{a,b\in\mathbb{Z}>0\\1\leq ab\leq x}}\frac{1}{(ab)^3}aJ_2(a)$$

$$=\frac{1}{x}\sum_{\substack{a,b\in\mathbb{Z}>0\\1\leq ab\leq x}}\frac{1}{b^3}\frac{1}{a^2}J_2(a)=\frac{1}{x}\sum_{1\leq b\leq x}\frac{1}{b^3}\sum_{1\leq a\leq\frac{x}{b}}\frac{1}{a^2}J_2(a)$$

where a and b are positive integers, such that $ab=n$.

Thus from $J_2(n)=\sum_{d|n}\mu(d)\left(\frac{n}{d}\right)^2$ we get

$$\sum_{1\leq a\leq\frac{x}{b}}\frac{1}{a^2}J_2(a)=\sum_{1\leq a\leq\frac{x}{b}}\frac{1}{a^2}\sum_{d|a}\mu(d)\left(\frac{a}{d}\right)^2$$

$$=\sum_{1\leq a\leq\frac{x}{b}}1\sum_{d|a}\frac{1}{d^2}\mu(d)=\sum_{\substack{d,d'\in\mathbb{Z}>0\\dd'\leq\frac{x}{b}}}\frac{\mu(d)}{d^2}$$

$$=\sum_{1\leq d\leq\frac{x}{b}}\frac{\mu(d)}{d^2}\sum_{1\leq d'\leq\frac{x}{db}}1=\sum_{1\leq d\leq\frac{x}{b}}\frac{\mu(d)}{d^2}\cdot\frac{x}{db}=\frac{x}{b}\sum_{1\leq d\leq\frac{x}{b}}\frac{\mu(d)}{d^3}.$$

Taking the limits we have

$$\lim_{x\to\infty}\frac{1}{x}\sum_{1<n\leq x}\frac{1}{n^3}\sum_{d|n}dJ_2(d)$$

$$=\lim_{x\to\infty}\frac{1}{x}\sum_{1<b\leq x}\frac{1}{b^3}\sum_{1\leq a\leq\frac{x}{b}}\frac{1}{a^2}J_2(a)$$

$$= \lim_{x\to\infty} \frac{1}{x} \sum_{1\le b\le x} \frac{1}{b^3} \cdot \frac{x}{b} \sum_{1\le d\le \frac{x}{b}} \frac{\mu(d)}{d^3}$$

$$= \lim_{x\to\infty} \sum_{1\le b\le x} \frac{1}{b^4} \sum_{1\le d\le \frac{x}{b}} \frac{\mu(d)}{d^3}$$

$$= \sum_{b=1}^{\infty} \frac{1}{b^4} \cdot \sum_{d=1}^{\infty} \frac{\mu(d)}{d^3}.$$

Now, $\sum_{b=1}^{\infty} \frac{1}{b^4} = \zeta(4)$ and $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^3} = \frac{1}{\zeta(3)}$ from Theorem 4.9. Thus we get the result. □

For the other terms, we give the following Lemma that will help us to determine the limit.

LEMMA 5.7. $\sum_{n=1}^{x} \frac{1}{n} \le \log(x) + 1.$

PROOF. By the integral test from calculus we have

$$\sum_{n=2}^{\infty} \frac{1}{n} \le \int_1^x \frac{1}{u} du,$$

and so

$$\sum_{n=1}^{\infty} \frac{1}{n} \le \int_1^x \frac{1}{u} du + 1 = \log(u) \,|_1^x + 1 = \log(x) + 1.$$

□

Thus for large x we have

$$\sum_{n=1}^{x} \frac{1}{n} \le 2\log(x).$$

LEMMA 5.8. $\lim_{x\to\infty} \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d) = 0.$

PROOF. Note that for $n > 1$,

$$\frac{1}{n^3(n-1)} \leq \frac{1}{n^3\left(n-\frac{n}{2}\right)} = \frac{2}{n^4}$$

Thus we have

$$0 < \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d)$$

$$\leq \frac{1}{x} \sum_{1<n\leq x} \frac{2}{n^4} \sum_{d|n} dJ_2(d).$$

Applying the same argument as in Lemma 5.7, we have

$$\frac{1}{x} \sum_{1<n\leq x} \frac{2}{n^4} \sum_{d|n} dJ_2(d) \leq \frac{2}{x} \sum_{\substack{a,b\in\mathbb{Z}>0 \\ 1<ab\leq x}} \frac{1}{(ab)^4} aJ_2(a)$$

$$= \frac{2}{x} \sum_{\substack{a,b\in\mathbb{Z}>0 \\ 1<ab\leq x}} \frac{1}{b^4} \cdot \frac{1}{a^3} J_2(a)$$

$$= \frac{2}{x} \sum_{b=1}^{x} \frac{1}{b^4} \sum_{1<a\leq \frac{x}{b}} \frac{1}{a^3} J_2(a).$$

where a and b are positive integers, such that $ab = n$.

By the expression that we obtained for $J_2(a)$,

$$\sum_{1<a\leq \frac{x}{b}} \frac{1}{a^3} J_2(a)$$

$$= \sum_{1<a\leq \frac{x}{b}} \frac{1}{a} \sum_{d|a} \frac{1}{d^2} \mu(d)$$

as $d|a$ then set $a = dd'$. Then $1 \leq dd' \leq \frac{x}{b}$ so $1 \leq d' \leq \frac{x}{db}$. Thus we get,

$$= \sum_{1\le d\le \frac{x}{b}} \frac{1}{d^2}\mu(d) \sum_{1\le d'\le \frac{x}{bd}} \frac{1}{d'}.$$

By Lemma 5.7, for large x we have,

$$\sum_{1\le d'\le \frac{xb}{d}} \frac{1}{d'} \le 2\log\left(\frac{x}{bd}\right).$$

Therefore,

$$\sum_{1<a\le \frac{x}{b}} \frac{1}{a^3} J_2(a) \le \sum_{1\le d\le \frac{x}{b}} \frac{1}{d^2}\mu(d) 2\log\left(\frac{x}{bd}\right)$$

$$= 2\log(x) \sum_{1\le d\le \frac{x}{b}} \frac{1}{d^2}\mu(d) - 2\sum_{1\le d\le \frac{x}{b}} \frac{\log(db)}{d^2}\mu(d)$$

$$\le 2\log(x) \sum_{1\le d\le \frac{x}{b}} \frac{1}{d^2}\mu(d).$$

Thus,

$$\lim_{x\to\infty} \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d)$$

$$\le \lim_{x\to\infty} \frac{1}{x} \sum_{1<n\le x} \frac{2}{n^4} \sum_{d|n} dJ_2(d)$$

$$= \lim_{x\to\infty} \frac{2}{x} \sum_{1\le b\le x} \frac{1}{b^4} \sum_{1<a\le \frac{x}{b}} \frac{1}{a^3} J_2(a)$$

$$\le \lim_{x\to\infty} \frac{2}{x} \sum_{1\le b\le x} \frac{1}{b^4} 2\log(xb) \sum_{1\le d\le \frac{x}{b}} \frac{1}{d^2}\mu(d).$$

This is

$$\le \lim_{x\to\infty} \frac{2\log(x)}{x} \sum_{1\le b\le x} \frac{1}{b^4} \sum_{1\le d\frac{x}{b}} \frac{1}{d^2}\mu(d)$$

$$= \lim_{x\to\infty} \frac{2\log(x)}{x} \sum_{b=1}^{\infty} \frac{1}{b^4} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$$

$$= \lim_{x\to\infty} \frac{2\log(x)}{x} \cdot \zeta(4) \cdot \frac{1}{\zeta(2)}.$$

Now,

$$\lim_{x\to\infty} \frac{\log(x)}{x} = \lim_{x\to\infty} \frac{\frac{1}{x\ln 10}}{1} = \lim_{x\to\infty} \frac{1}{x\ln 10} = 0$$

by L'Hopital's Rule, and the expression above is 0. □

We now consider the last term.

LEMMA 5.9. $\lim_{x\to\infty} \frac{1}{x} \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d) = 0.$

PROOF. For $n > 1$, $\frac{1}{n^2(n-1)} \le \frac{2}{n^3}$, so we have

$$0 \le \sum_{1<n\le x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d)$$

$$\le \sum_{1<n\le x} \frac{2}{n^3} \sum_{d|n} d\phi(d)$$

$$= \sum_{\substack{a,b\in\mathbb{Z}>0 \\ 1<ab\le x}} \frac{2}{(ab)^3} a\phi(a) \le 2 \sum_{1\le b\le x} \frac{1}{b^3} \sum_{1\le a\le \frac{x}{b}} \frac{\phi(a)}{a^2}.$$

From Lemma 4.8 we have

$$\frac{\phi(a)}{a^2} = \frac{1}{a} \sum_{d|1} \frac{\mu(d)}{d}.$$

Thus,

$$\begin{aligned}
\sum_{1\le a\le \frac{x}{b}} \frac{\phi(a)}{a^2} &= \sum_{1\le a\le \frac{x}{b}} \frac{1}{a}\sum_{d|a}\frac{\mu(d)}{d} \\
&= \sum_{\substack{d,d'\in\mathbb{Z}>0 \\ 1\le dd'\le \frac{x}{b}}} \frac{1}{d'}\cdot\frac{\mu(d)}{d} \\
&= \sum_{1\le d\le \frac{x}{b}} \frac{\mu(d)}{d}\sum_{1\le d'\le \frac{x}{bd}}\frac{1}{d'} \\
&\le \sum_{1\le d\le \frac{x}{b}} \frac{\mu(d)}{d}\log\left(\frac{x}{bd}\right) \le \log(x)\sum_{1\le d\le \frac{x}{b}}\frac{\mu(d)}{d}
\end{aligned}$$

from the same argument as in Lemma 5.9. Thus,

$$0 \le \lim_{x\to\infty}\frac{1}{x}\sum_{1<n\le x}\frac{1}{n^2(n-1)}\sum_{d|n} d\phi(d)$$

$$\le \lim_{x\to\infty}\frac{2}{x}\sum_{1\le b\le x}\frac{1}{b^3}\log(x)\sum_{1\le d\le \frac{x}{b}}\frac{\mu(d)}{d}$$

$$= \lim_{x\to\infty}\frac{2\log(x)}{x}\sum_{b=1}^{\infty}\frac{1}{b^3}\lim_{x\to\infty}\sum_{1\le d\le \frac{x}{2}}\frac{\mu(d)}{d}$$

$$= 2\zeta(3)\lim_{x\to\infty}\frac{\log(x)}{x}\lim_{x\to\infty}\sum_{1\le d\le \frac{x}{2}}\frac{\mu(d)}{d}$$

$$= 2\zeta(3)\lim_{x\to\infty}\frac{\log(x)}{x}\lim_{x\to\infty}\sum_{1\le d\le \frac{x}{2}}\frac{\mu(d)}{d}$$

$$\le 2\zeta(3)\lim_{x\to\infty}\frac{\log(x)}{x}\lim_{x\to\infty}\sum_{1\le d\le \frac{x}{2}}\frac{1}{d}$$

because $\mu(d) = 0, 1$, or -1. Thus we get,

$$\le 2\zeta(3)\lim_{x\to\infty}\frac{2\left(\log(x)\right)^2}{x}$$

$$\leq \lim_{x\to\infty} \frac{2\log(x)}{x} \cdot \zeta(3) \sum_{1\leq d\leq \frac{x}{b}} \frac{1}{d}$$

$$\leq \lim_{x\to\infty} \frac{4\left(\log(x)\right)^2}{x} \cdot \zeta(3).$$

From L'Hopital's Rule we have

$$\lim_{x\to\infty} \frac{\left(\log(x)\right)^2}{x} = \lim_{x\to\infty} \frac{2\log(x)}{x} = 2 \lim_{x\to\infty} \frac{1}{x\ln 10} = 0.$$

Thus we get the result. □

Putting all of these terms together we get

$$\lim_{x\to\infty} \frac{1}{x} \sum_{1<n\leq x} \frac{E_2(C_n)}{n} =$$

$$\lim_{x\to\infty} \left[\frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^3} \sum_{d|n} dJ_2(d) + \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d) - \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d) \right]$$

$$=$$

$$\lim_{x\to\infty} \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^3} \sum_{d|n} dJ_2(d) + \lim_{x\to\infty} \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^3(n-1)} \sum_{d|n} dJ_2(d) - \lim_{x\to\infty} \frac{1}{x} \sum_{1<n\leq x} \frac{1}{n^2(n-1)} \sum_{d|n} d\phi(d)$$

$$= \frac{\zeta(4)}{\zeta(3)} + 0 - 0$$

$$= \frac{\zeta(4)}{\zeta(3)}$$

by applying Lemma 5.7, Lemma 5.8, Lemma 5.9. This proves Theorem 2.

Chapter 6

Conclusion and Future Work

We introduced a new concept for the study of groups, the expectation numbers $E_k(G)$. These numbers can be used to study the sizes of subgroups of the group G which are generated by randomly chosen elements of the group G. How likely randomly chosen elements of G generate G is a subject of much study. We then showed some basic computations of $E_k(G)$ for small k and certain groups G. We proved some results about $E_1(G)$ and $E_2(G)$ for cyclic groups G. In particular, we have applied number-theoretic methods to study certain properties of cyclic groups. In particular, we showed asymptotic properties of the 1^{st} and 2^{nd} expectation numbers of cyclic groups. The results here can be extended several ways.

First, the methods used to prove Theorem 1 and Theorem 2 are very similar. Therefore, it seems that we can further extend these methods to prove results about $E_k(C_n)$, for general k. We conjecture that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{1\leq n\leq x} \frac{E_k(C_n)}{n} = \frac{\zeta(k+2)}{\zeta(k+1)}.$$

The main idea to prove the above result will be to obtain an expression for $E_k(C_n)$ in terms of arithmetic functions. It seems that, as in the cases for $E_1(C_n)$ and $E_2(C_n)$, we should be able to express $E_k(C_n)$ as a sum of Jordan's Totient Functions, $J_1(n), J_2(n) \dots J_k(n)$. Then similar analyses as done in Chapters 4 and 5 should give the above result.

Second, we can apply similar, and other methods to study the expectation numbers of different groups. In particular, the results of Dixon [**7**] can be expressed in terms of

$E_2(S_n)$. That is, the results in [**7**] give $\lim_{n\to\infty} E_2(S_n) = 1$ or $\frac{1}{2}$. Similar results of Dixon of Erdős and Turán imply results about such expectation numbers. We can study $E_k(S_n)$ for symmetric groups S_n. Further, we can study $E_k(D_n)$ for dihedral groups D_n or other groups.

Finally, we can study more carefully the growth and error terms of the asymptotic estimates given here and in other papers, such as Dixon [**6, 7**] and Erdős and Turán [**9, 10, 11, 12, 13, 14, 15**].

BIBLIOGRAPHY

[1] H. Amiri, S.M. Jafarian Amiri, I.M. Isaacs, *Sums of Element Orders in Finite Groups,* Comm. Algebra. **37** no. 9, 9(2009), 2978-2980.

[2] R. Apéry, *Irrationalité de* $\zeta(2)$ *et* $\zeta(3)$, Astérisque **61**, 11-13, 1979.

[3] L. Babai, *The Probability of Generating the Symmetric Group*, J. Combin. Theory Ser. A 52 no.1 (1989), 148-153.

[4] L. Babai and T.P. Hayes, *The probability of generating the symmetric group when one of the generators is random,* Publ. Math. Debrecen 69 no. 3 (2006), 271-280.

[5] K. Ball and T. Rivoal, *Irrationalité d'une infinité valeurs de la fonction zêta aux entiers impairs*, Invent. Math. **146**, 193-207, 2001.

[6] J.D. Dixon, *The probability of generating the symmetric group,* Math. Z. 110 (1969), 199-205.

[7] J.D. Dixon, *Random sets which invariably generate the symmetric group,* Discrete Math. 105 (1992), 25-39.

[8] J.D. Dixon, *Asymptotics of generating the symmetric and alternating groups,* Electron. J. Combin. 12 (2005), Research Paper 56.

[9] P. Erdős and P. Turán, *On some problems of a statistical group-theory.* I. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **4**, (1965), 175-186.

[10] P. Erdős and P. Turán, *On some problems of a statistical group-theory. II.* Acta math. Acad. Sci. Hungar. **18** (1967), 151-163.

[11] P. Erdős and P. Turán, *On some problems of a statistical group-theory. III.* Acta math. Acad. Sci. Hungar. **18** (1967), 309-320.

[12] P. Erdős and P. Turán, *On some problems of a statistical group-theory. IV.* Acta math. Acad. Sci. Hungar. **19** (1968), 413-435.

[13] P. Erdős and P. Turán, *On some problems of a statistical group-theory. VI.* J. Indian Math. Soc. 34 (1970), no. 3-4, 175-192.

[14] P. Erdős and P. Turán, *On some problems of a statistical group-theory. V.* Period. Math. Hungar. 1, no. 1, (1971), 5-13.

[15] P. Erdős and P. Turán, *On some problems of a statistical group-theory. V.* Period. Math. Hungar. 2, (1972), 149-163.

[16] J. Gallian, *Contemporary Abstract Algebra,* 6^{th} *ed.,* Houghton Mifflin Company, 2006.

[17] J. Gathen, A. Knopfmacher, F. Luca, L.G. Lucht, and I.E. Shparlinski, *Average order in cyclic groups,* J. de Théorie des Nombres de Bordeaux. **16**, (2004), 107-123.

[18] H.W. Gould and T. Shonhiwa, *Functions of GCD's and LCM's,* Indian J. Math. 39 no. 1 (1997), 11-35.

[19] H.W. Gould and T. Shonhiwa, *A generalization of Cesàro's function and other results,* Indian J. Math. 39 no. 2 (1997), 183-194.

[20] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers,* 6^{th} *ed.*, Oxford Univ. Press, 2008.

[21] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloquium Publications, **53**, 2004.

[22] J.P. McCarthy, *Introduction to Arithmetical Functions*, Springer-Verlag New York Inc, 1986.

[23] I. Niven, H. S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers,* 5^{th} *ed.*, John Wiley&Sons Inc, 1991.

[24] T. Rivoal, *Irrationalité d'au moins un des neuf nombres* $\zeta(5), \zeta(7) \ldots \zeta(21)$, Acta Arith. **103** (2001), no. 2, 157-167

[25] T. Rivoal, *La fonction ẑeta de Riemann prend une infinité de valeurs rationnelles aux entiers impairs*, C.R. Acad. Sci Pari Sér I. Math 331 (2000) no. 4, 267-270.

[26] N.J.A. Sloane, *The On-line Encyclopedia of Integer Sequences.* (2015, July 13). Retrieved from www.oeis.org