Proceedings of The National Conference
On Undergraduate Research (NCUR) 2013
University of Wisconsin La Crosse, WI
April 11 - 13, 2013

Prime Numbers and the Convergents of a Continued Fraction

Cahlen Humphreys
The Department of Mathematics
Boise State University
1910 University Drive
Boise, Idaho 83725 USA

Faculty Advisor: Dr. Liljana Babinkostova

Abstract

Continued fractions offer a concrete representation of arbitrary real numbers, where in the past such numbers were represented in decimal format. Continued fractions are found useful in many different areas of mathematics and science. Since ancient times they have played an important role in the approximation to real numbers by rational numbers, using convergents. In 1939 P. Erdos and K. Mahler showed that there are irrational numbers for which each of the denominators of the convergents of their continued fraction expansion is a prime number. Using the techniques presented in their paper, and through Theorem 3.5 and Corollary 3.6, we show that *for almost all* real numbers the greatest prime factor of the numerator of the n^{th} convergent of the corresponding continued fraction increases rapidly with n.

Keywords: Continued Fractions, Convergents, Prime Numbers

1. Introduction

The first appearance of a continued fraction is often difficult to pinpoint with complete accuracy because they have been used extensively throughout the past 2000 years. However, the origins of the continued fraction are generally placed at the advent of the Euclidean Algorithm. The term *continued fraction* was first coined by the mathematician John Wallis in his book *Opera Mathematica* in 1693. In his book he was also the first to explain what the n^{th} convergent of a continued fraction was and how to compute it (Definition 1.3). Applications of continued fractions can be witnessed in mathematical cryptography, atomic physics, cosmological models, and ecology (see eg. [7], [5], [6], and [15]). Cryptography is a tool that helps information security meet many of its goals. Through cryptography two parties can exchange private data in a public manner without the threat of a third-party compromising the integrity of the data. There are many types of cryptosystems (see eg. [7], [8], [13]) in which their security relies on a computationally difficult mathematical problem. One such cryptosystem relies on a factoring problem to ensure security [7], and several factoring algorithms based on continued fractions have been developed that defeat the security of this cryptosystem (see eg. [3], [9]).

Definition 1.1 A continued fraction is of the form

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}} = \underbrace{a_0 + \left\lfloor \frac{b_0}{a_1} \right\rfloor + \left\lfloor \frac{b_1}{a_2} \right\rfloor + \cdots}_{\text{Alternate Notation}},$$

where $a_0, a_1, a_2, \ldots$ and $b_0, b_1, \ldots$ may be real or complex numbers. A Simple Continued Fraction is of the same form except $b_0 = b_1 = b_2 = \cdots = 1$, a_0 is either positive, negative, or zero, and $a_1, a_2, \ldots$ are all positive integers. We also use $[a_0, a_1, a_2, a_3, \ldots]$ as an alternate notation for a simple continued fraction where $a_0, a_1, a_2, \ldots$ are called partial quotients.

Theorem 1.2[2] A number is rational if and only if it can expressed as a simple finite continued fraction. Conversely, a number is irrational if and only if it can be expressed as an simple infinite continued fraction.

Definition 1.3[12] The continued fraction $[a_1; a_2, a_3, \ldots, a_n]$ where n is a non-negative integer less than or equal to k is called the n^{th} convergent of the continued fraction $[a_1; a_2, a_3, \ldots, a_k]$. The n^{th} convergent is denoted by C_n.

Theorem 1.4[1] The numerators A_n and the denominators B_n of the n^{th} convergent C_n of the continued fraction $[a_1, a_2, \ldots, a_k]$ satisfy the equations

$$A_n = a_n A_{n-1} + A_{n-2},$$
$$B_n = a_n B_{n-1} + B_{n-2},$$

where $(n = 3, 4, 5, \ldots, k)$, with the initial values $A_1 = a_1,\ A_2 = a_2 a_1 + 1,\ B_1 = 1,$ and $B_2 = a_2$.

For example, $C_1 = A_1/B_1 = 1,\ C_2 = A_2/B_2 = 3/2,\ C_3 = A_3/B_3 = 10/7$ are convergents of the continued fraction $1 + \frac{1|}{|2} + \frac{1|}{|3}$.

Theorem 1.5[14] Let x be irrational, then there are infinitely many rationals numbers $\frac{A}{B}$ such that

$$\left| x - \frac{A}{B} \right| \leq \frac{1}{B^2}.$$

Backdoors are common in cryptosystems as an easy way to retrieve data if a private key is lost. One such RSA backdoor [10] can be broken using Theorem 1.5 with continued fractions [11].

Theorem 1.6[14] Let x be irrational, and let $\frac{A}{B}$ be a rational in lowest terms with $B > 0$, suppose that

$$\left| x - \frac{A}{B} \right| \leq \frac{1}{2B^2}.$$

Then $\frac{A}{B}$ is a convergent in the continued fraction expansion of x.

Given an integer n, we denote the greatest prime factor of n as $G(n)$. In [4], P. Erdos and K. Mahler showed the following result:

Theorem 1.7[4] The set of all irrational numbers ζ in $0 \leq \zeta \leq 1$, for which an infinity of indices n exist satisfying

$$G(B_n) \leq e^{\frac{\ln B_n}{20 \ln \ln B_n}}$$

is of measure zero, where B_n is the denominator of the n^{th} convergent of the continued fraction expansion of ζ.

We show that Theorem 1.7 is also valid for the numerator A_n.

In [4], P. Erdos and K. Mahler showed the following:

Theorem 1.8[4] For almost all irrational numbers ζ, the greatest prime factor of the denominator of the n^{th} convergent of the continued fraction expansion of ζ, increases rapidly with n.

In this paper we show a corresponding result, except with respect to the numerator of the n^{th} convergent of the continued fraction expansion of ζ, by Corollary 3.6.

In Section 2 we introduce and define Big O Notation which is essential for the majority of our theorems. In Section 3 we follow the techniques established by P. Erdos and K. Mahler in their paper [4], however we fill in a number of gaps that were orignially left out by the authors. Additionally, in Section 3 we prove Theorem 3.5, which is paramount concerning the validity of Corollary 3.6. Section 4 is comprised of data analysis where we applied our research with concrete numbers. Through this analysis we stray a bit and find that investigating convergents with both prime numerators and prime denominators could be an insightful area for future research.

2. Big O Notation

Big O Notation, also called Landau's Symbol, is a symbol in mathematics and computer science that is used to describe the asymptotic nature of functions. Throughout this paper we will make use of Big O Notation.

Definition 2.1[16] Suppose $f(x)$ and $g(x)$ are two functions defined on a subset of the real numbers, we write $f(x) = \mathcal{O}(g(x))$ if an only if there exists constants N and C such that $|f(x)| \leq C|g(x)|$ for all $x > N$.

Theorem 2.2[16] If $f_1(x) = \mathcal{O}(g_1(x))$ and $f_2(x) = \mathcal{O}(g_2(x))$, then $f_1(x) + f_2(x) = \mathcal{O}(\max(g_1(x), g_2(x)))$.

Theorem 2.3[16] If $f_1(x) = \mathcal{O}(g_1(x))$ and $f_2(x) = \mathcal{O}(g_2(x))$, then $f_1(x) \cdot f_2(x) = \mathcal{O}(g_1(x) \cdot g_2(x))$.

3. Irrational numbers and convergents with prime numbers

Let A_n/B_n be the n^{th} convergent of an infinite continued fraction $\zeta = [a_1, a_2, a_3, \dots]$ where $a_1, a_2, \dots$ are positive integers. We show that for *almost all* ζ, $G(A_n)$ increases rapidly with n. In the following, ζ is a positive irrational number where

$$\frac{A_{-1}}{B_{-1}} = \frac{1}{0}, \qquad \frac{A_0}{B_0} = \frac{a_0}{1}, \qquad \frac{A_1}{B_1} = \frac{a_0a_1 + 1}{a_1}, \qquad \dots$$

is the sequence of its convergents. We divide the set of all positive integers k for which

$$k \leq x, \qquad G(k) \leq e^{\frac{\ln k}{20 \ln(\ln k)}} \tag{1}$$

into three classes H, I, and J. Where H consists of those elements which are divisible by a square greater than or equal to $(\ln x)^{10}$, and the remaining elements k belong to I or J, according as $k \geq \sqrt{x}$ or $k < \sqrt{x}$. Let $L = e^{\frac{\ln k}{20 \ln \ln k}}$, $S = \{\xi < k : G(k) \leq L\}$ and $T_x = \{k \leq x : G(k) \leq L\}$. Let

$$\begin{aligned} H &= \{k \in T_x : (\exists r \in \mathbb{N})(r^2 \geq (\ln x)^{10} \text{ and } r^2|k)\}, \\ I &= \{k \in T_x - H : k \geq \sqrt{x}\}, \\ J &= \{k \in T_x - (H \cup I) : k < \sqrt{x}\}, \end{aligned}$$

then $S = \cup T_x$. We now prove three lemmas that show us the size of H, I, and J, which we will need to prove Theorem 3.4.

Lemma 3.1 If $H = \{k \in T_x : (\exists r \in \mathbb{N})(r^2 \geq (\ln x)^{10} \text{ and } r^2|k)\}$, then $|H| = \mathcal{O}\left(\frac{x}{(\ln x)^5}\right)$.

Proof. The object is to find how many multiples r^2 there are of k that are less than x but greater than $(\ln x)^{10}$. Observe that there are x/r^2 many multiples less than or equal to x. Since $r^2 \geq (\ln x)^{10}$, then certainly $r \geq (\ln x)^5$. Therefore,

$$|H| = \sum_{r \geq (\ln x)^5} \frac{x}{r^2} = x \sum_{r \geq (\ln x)^5} \frac{1}{r^2} = x \int_{(\ln x)^5}^{\infty} \frac{1}{y^2} dy = x \lim_{y \to \infty} \int_{(\ln x)^5}^{y} \frac{1}{y^2} dy = x \left(\lim_{y \to \infty} -\frac{1}{y} + \frac{1}{(\ln x)^5} \right) = \frac{x}{(\ln x)^5}.$$

This implies that $|H| \leq x/(\ln x)^5$, and in Big O notation we have $|H| = \mathcal{O}\left(x/(\ln x)^5\right)$. □

Lemma 3.2 If $I = \{k \in T_x - H : k \geq \sqrt{x}\}$, then $|I| = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right)$.

Proof. To find $|I|$ let $k \in I$, and let $k = p_1^{h_1} p_2^{h_2} p_3^{h_3} \dots p_t^{h_t}$ be its representation as a product of powers of different primes. Since $k \in I$, then

$$\sqrt{x} \leq k \leq x. \tag{2}$$

If an exponent $h \geq 2$, either p^{h-1} or p^h is a square factor of k, and therefore $p^{h-1} < (\ln x)^{10}$. There are two cases, either h is even or h is odd. If h is odd then $h = 2\ell + 1$ for some integer ℓ, and we have $p^{h-1} = p^{2\ell+1-1} = p^{2\ell}$, thus

a square factor fo k. If h is even, then it is plain that p^h is a square factor of k, and $p^{h-1} < (\ln x)^{10}$ holds. We are looking at elements in I, so all square factors will be less than $(\ln x)^{10}$ since we have already accounted for all square factors greater than or equal to $(\ln x)^{10}$ when determining the size of H. Since $p^{h-1} < (\ln x)^{10}$, then it must be that $p^h \leq (\ln x)^{\frac{10h}{h-1}}$, and since it is the case that $h \geq 2$ then $(\ln x)^{\frac{10h}{h-1}} \leq (\ln x)^{20}$.

Note that since $\lim\limits_{x\to\infty} \dfrac{\ln x}{(\ln(\ln x))^2} = \infty$, we observe that for sufficiently large x,

$$800 \leq \frac{\ln x}{(\ln(\ln x))^2} \implies 20 \leq \frac{\ln x}{40(\ln(\ln x))^2} \implies 20 \cdot \ln(\ln x) \leq \frac{\ln x}{40(\ln(\ln x))}. \tag{3}$$

Thus, we end up with

$$20 \cdot \ln(\ln x) \leq \frac{\ln x}{40(\ln(\ln x))} \implies e^{\ln(\ln x)\cdot 20} \leq e^{\frac{\ln x}{40\ln(\ln x)}} \implies (\ln x)^{20} \leq e^{\frac{\ln x}{40\ln(\ln x)}}. \tag{4}$$

Now observe that

$$e^{\frac{\ln x}{40\ln(\ln x)}} = e^{\frac{\ln x}{20(\ln(\ln x))}\cdot\frac{1}{2}} = e^{\frac{\frac{1}{2}\cdot\ln x}{20(\ln(\ln x))}} = e^{\frac{\ln\sqrt{x}}{20(\ln(\ln x))}}, \tag{5}$$

and since $\sqrt{x} \leq k \leq x$,

$$20\ln(\ln k) < 20\ln(\ln x) \implies \frac{1}{20\ln(\ln x)} < \frac{1}{20\ln(\ln k)} \tag{6}$$

then we have that

$$e^{\frac{\ln\sqrt{x}}{20\ln(\ln x)}} \leq e^{\frac{\ln k}{20\ln(\ln(k))}}. \tag{7}$$

Lastly, because of (2) through (7) we have that $p^h \leq (\ln x)^{\frac{10h}{h-1}} \leq (\ln x)^{20} \leq e^{\frac{\ln x}{40(\ln(\ln x))}} \leq e^{\frac{\ln k}{20\ln(\ln k)}}$. When $h = 1$ we have that $k = p_1 p_2 \cdots p_t$ where $t \geq 20\ln(\ln k)$. Thus, we have that k is divisible by at least $20\ln(\ln k)$ distinct primes. Further, observe that since $\sqrt{x} \leq k$ we have

$$\begin{aligned}&\frac{1}{2}\ln x \leq \ln k \implies \ln x \leq 2\cdot\ln k \implies \ln(\ln x) \leq \ln(2\cdot\ln k) \implies 10\cdot\ln(\ln x) \leq 10\cdot\ln(2\cdot\ln k)\\ &\implies 10\cdot\ln(\ln x) \leq 10\cdot\ln(2\cdot\ln k) \leq 10\cdot\ln((\ln k)^2) = 20\cdot\ln(\ln k)\end{aligned}$$

therefore it must be that $10\cdot\ln(\ln x) \leq 20\cdot\ln(\ln k)$. So we find that k is divisible by at least $20\ln(\ln k) \geq 10\ln(\ln x)$ different prime factors for sufficently large x. Denote $d(k)$ as the the total number of divisors of k, then by definition of the divisor function $\sigma(p_n\#) = 2^n$, where $p_n\#$ is the primorial of k. It follows that

$$d(k) = \sigma(p_t\#) = 2^t = \underbrace{2\cdot 2\cdot 2\cdot\cdots\cdot 2}_{t \geq 10\ln(\ln x)}$$

and from this we have that

$$d(k) \geq 2^{10\ln(\ln x)} = (2^2)^{5\ln(\ln x)} \geq e^{\ln((\ln x)^5)} = (\ln x)^5.$$

By Dirichlet we have $\sum_{k\leq x} d(k) = \mathcal{O}(x\ln x)$, and since $d(k) \geq (\ln x)^5 \implies \frac{x\ln x}{d(k)} \leq \frac{x\ln x}{(\ln x)^5}$ it must be that I has at most

$$\frac{1}{(\ln x)^5}\mathcal{O}(x\ln x) = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right)$$

elements k. □

Lemma 3.3 If $J = \{k \in T_x - (H \cup I) : k < \sqrt{x}\}$, then $|H| + |I| + \sqrt{x} = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right)$.

Proof. By Lemma 3.1 and Lemma 3.2, and since J has less than $\sqrt{x}$ elements, there are therefore only

$$\mathcal{O}\left(\frac{x}{(\ln x)^5}\right) + \mathcal{O}\left(\frac{x}{(\ln x)^4}\right) + \sqrt{x} \tag{8}$$

integers k satisfying (1). We can write (8) as $C_1\frac{x}{(\ln x)^5} + C_2\frac{x}{(\ln x)^4} + C_3\sqrt{x}$ and take $C = \max\{C_1, C_2, C_3\}$, then

$$\begin{aligned} &C_1\frac{x}{(\ln x)^5} + C_2\frac{x}{(\ln x)^4} + C_3\sqrt{x} \le C\left(\frac{x}{(\ln x)^4} + \frac{x}{(\ln x)^4} + x\right) = C\left(\frac{2x + x(\ln x)^4}{(\ln x)^4}\right) \le C\left(\frac{2x + 2x(\ln x)^4}{(\ln x)^4}\right) \\ &= 2C\left(\frac{x + x(\ln x)^4}{(\ln x)^4}\right) \le C\left(\frac{x(1 + \frac{1}{x^4})}{(\ln x)^4}\right) \le C\left(\frac{2x}{(\ln x)^4}\right) = 2C\left(\frac{x}{(\ln x)^4}\right) = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right). \end{aligned} \tag{9}$$

Therefore by (9) we have that

$$|H| + |I| + \sqrt{x} = \mathcal{O}\left(\frac{x}{(\ln x)^5}\right) + \mathcal{O}\left(\frac{x}{(\ln x)^4}\right) + \sqrt{x} = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right).$$

□

The following theorem will be used to help us prove our main result. It follows (Lemma 1, [4]) by P. Erdos and K. Mahler, however we give a much more detailed account.

Theorem 3.4[4] Let S be the set of all positive integers k for which

$$k \ge \xi, \qquad G(k) \le e^{\frac{\ln k}{20\ln(\ln k)}}$$

then, for large $\xi > 0$,

$$\sum_{k\in S}\frac{1}{k} = \mathcal{O}\left((\ln \xi)^{-3}\right).$$

Proof. Suppose now that

$$k_1, k_2, k_3, \ldots, k_i, \ldots \qquad (1 \le k_1 < k_2 < k_3 < \ldots)$$

is a sequence of positive integers for which $G(k_i) \le e^{\frac{\ln k}{20\ln(\ln k)}}$. We have shown through Lemma 3.1, Lemma 3.2, and Lemma 3.3 that $|T| = |A| + |B| + |C| = \mathcal{O}\left(\frac{x}{(\ln x)^4}\right)$, so consider the case that T contains only one element k_1, where $k_1 \ge 1$. We have $1 = |T| = \mathcal{O}\left(\frac{k_1}{(\ln k_1)^4}\right)$ and therefore $\frac{1}{k_1} \le C\frac{1}{(\ln k_1)^4}$. Consider the case that T contains two elements k_1 and k_2 where $k_1 < k_2$ and $k_2 \ge 2$. We have $2 = |T| = \mathcal{O}\left(\frac{k_2}{(\ln k_2)^4}\right)$ and therefore $\frac{1}{k_2} \le C\frac{1}{2(\ln k_2)^4}$. Lastly, consider the case where T contains three elements k_1, k_2, k_3 where $k_1 < k_2 < k_3$ and $k_3 \ge 3$. We have $3 = |T| = \mathcal{O}\left(\frac{k_3}{3(\ln k_3)^4}\right)$ and therefore $\frac{1}{k_3} \le C\frac{1}{3(\ln k_3)^4}$. It follows that $\frac{1}{k_i} \le C\frac{1}{i(\ln k_i)^4}$. Now consider the summation for $1/k_i$ for $i \ge n$

$$\sum_{i\ge n}\frac{1}{k_i} = \mathcal{O}\left(\frac{1}{n(\ln n)^4}\right) + \mathcal{O}\left(\frac{1}{(n+1)(\ln(n+1))^4}\right) + \cdots = \mathcal{O}\left(\frac{1}{n(\ln n)^4}\right) \tag{10}$$

and by (10) we have

$$\sum_{i\ge n}\frac{1}{k_i} \le C\frac{1}{n(\ln n)^4} \le C\frac{1}{(\ln n)^4} \le C\frac{\ln n}{(\ln n)^4} = C\frac{1}{(\ln n)^3} \implies \sum_{i\ge n}\frac{1}{k_i} = \mathcal{O}\left(\frac{1}{(\ln n)^3}\right) \tag{11}$$

which completes our proof. □

The next theorem is original work. We need a way to utilize the techniques provided by P. Erdos and K. Mahler in [4], except with regard to the numerator instead of the denominator. Theorem 3.5 solves this quandary for us so that we can easily apply the techniques in [4].

Theorem 3.5 The n^{th} convergent of the simple continued fraction of the irrational number x where $0 \leq x \leq 1$, is the reciprocal to the n^{th} convergent of $1/x$.

Proof. We will use proof by induction. Let $x \in \mathbb{R}$ be irrational with $0 \leq x \leq 1$. Consider the simple continued fraction expansion for x,

$$x = 0 + \frac{1}{\lfloor a_1} + \frac{1}{\lfloor a_2} + \cdots = [0, a_1, a_2, \ldots].$$

We also have the simple continued fraction expansion for $1/x$ as

$$\frac{1}{x} = \frac{1}{0 + \frac{1}{\lfloor a_1} + \frac{1}{\lfloor a_2} + \cdots} = a_1 + \frac{1}{\lfloor a_2} + \cdots = [a_1, a_2, \ldots].$$

Let $c'_n = A'_n/B'_n$ represent convergents for x, and let $c_n = A_n/B_n$ represent convergents for $1/x$. For the first three convergents of c'_n we have,

$$A'_1 = 1, A'_2 = a_2, A'_3 = a_2a_3 + 1, \ldots$$
$$B'_1 = a_1, B'_2 = a_1a_2 + 1, B'_3 = a_1a_2a_3 + a_1a_3 + a_1, \ldots.$$

Similarly, for the first three convergents of c_n we have,

$$A_1 = a_1, A_2 = a_1a_2 + 1, A_3 = a_1a_2a_3 + a_1a_3 + a_1, \ldots$$
$$B_1 = 1, B_2 = a_2, B_3 = a_2a_3 + 1, \ldots.$$

Hence, we have that $A'_1 = B_1,\ A'_2 = B_2,$ and $A'_3 = B_3$. Consider the $n + 1^{th}$ convergent of x,

$$c'_{n+1} = 0 + \frac{1}{\lfloor a_1} + \frac{1}{\lfloor a_2} + \cdots + \frac{1}{\lfloor a_n} + \frac{1}{\lfloor a_{n+1}} = 0 + \frac{1}{\lfloor a_1} + \frac{1}{\lfloor a_2} \cdots + \frac{a_n a_{n+1} + 1}{\lfloor a_{n+1}}$$

which implies that by combining the last two terms of c'_{n+1} we get the equality

$$c'_{n+1} = \underbrace{[0, a_1, \ldots, a_{n-1}, a_n, a_{n+1}]}_{n+1^{th} \text{ convergent}} = \underbrace{[0, a_1, \ldots, a_{n-1}, \overbrace{\frac{a_n a_{n+1} + 1}{a_{n+1}}}^{n^{th} \text{ term}}]}_{n^{th} \text{ convergent}} = c'_n. \tag{12}$$

Since have have already shown that $A'_1 = B_1$, $A'_2 = B_2$, and $A'_3 = B_3$ then we have that

$$c'_1 = \frac{A'_1}{B'_1} = \frac{B_1}{A_1} = \frac{1}{\frac{A_1}{B_1}} = \frac{1}{c_1},$$

which satisfies the base case of our induction proof. For our inductive hypothesis assume that $c'_n = \frac{1}{c_n}$ for $n = k$.

Then for $n = k + 1$ we have that

$$\begin{aligned} c'_{k+1} &= [0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}] \\ &= \underbrace{\left[0, a_1, \ldots, a_{k-1}, \frac{a_k a_{k+1} + 1}{a_{k+1}}\right]}_{k^{th} \text{ convergent}} && \text{[By using (12).]} \\ &= \frac{1}{\left[a_1, a_2, \ldots, a_{k-1}, \frac{a_k a_{k+1}+1}{a_{k+1}}\right]} && \text{[By Inductive Hypothesis.]} \\ &= \frac{1}{[a_1, a_2, \ldots, a_k, a_{k+1}]} && \text{[By using (12).]} \\ &= \frac{1}{c_{k+1}}, \end{aligned}$$

and it is proved that for all $n \in \mathbb{N}$ we have $c'_n = 1/c_n$. □

Corollary 3.6 For almost all irrational numbers ζ, the greatest prime factor of the numerator A_n of the n^{th} convergent $C_n = A_n/B_n$ of the continued fraction expansion of ζ, increases rapidly with n.

Proof. By P. Erdos and K. Mahler (Lemma 2, [4]) and Theorem 3.5, we have that Theorem 1.7 holds for A_n. That is, we have that the set of all irrational numbers ζ in $0 \leq x \leq 1$, for which an infinity of indices n exist satisfying $G(A_n) \leq e^{\frac{\ln A_n}{20 \ln \ln A_n}}$ is of measure zero. Therefore, it follows from (Theorem 1, [4]) and (Theorem 1 (1), [4]) that for almost all ζ in $0 \leq \zeta \leq 1$ and all sufficiently large n we have that $G(A_n) \geq e^{\frac{n}{50 \ln n}}$. □

4. Experimental data

For a visual representation of our research we created the two graphs below. Using Maple we wrote a program that collected the number of prime numerators of convergents along with the largeness of the primes for a continued fraction expansion of a given irrational number. We tested convergents for $n \cdot e$ and $n \cdot \pi$ where $0 < n \leq 500$. For each n we then tested the primality of the the numerator for convergents up to 500 and 700, for $n \cdot e$ and $n \cdot \pi$ respectively. In two particular cases, $234 \cdot e$ (Figure 1) and $230 \cdot \pi$ (Figure 2) we found that indeed that number of prime numerators and the largeness of the primes increased as the convergents increased.

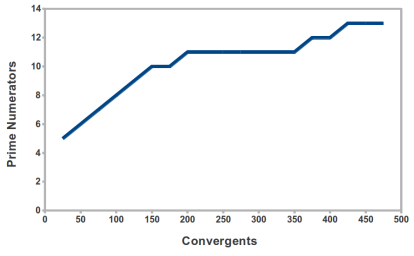

Figure 1: $(234 \cdot e)$ Prime Numerators vs Convergents

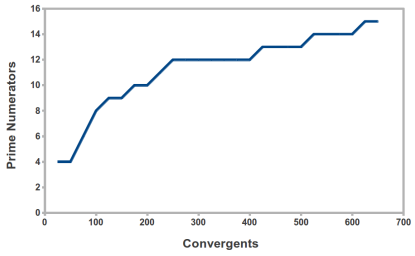

Figure 2: $(230 \cdot \pi)$ Prime Numerators vs Convergents

While collecting data for our experiment results, we also decided to collect data to determine the number of times that the convergents of e and π had both prime numerators and prime denominators. We found that by testing up to 2000 convergents for the continued fraction expansion of e there were only three such convergents that had both a prime numerator and denominator (Figure 3). Similarly, by testing up to 2000 convergents for the continued fraction expansion for π we only found one such case where a convergent had a prime numerator and denominator (Figure 4). In the future, we wish to explore the nature of irrational numbers where the convergents have both a prime numerator and denominator.

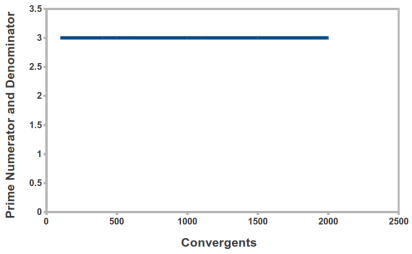

Figure 3: e Prime Numerator and Denominator vs Convergents

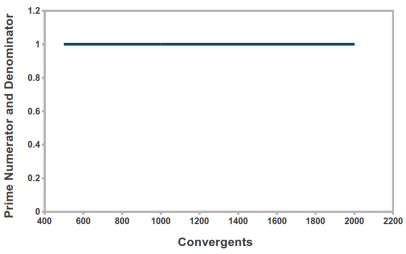

Figure 4: π Prime Numerator and Denominator vs Convergents

5. Concluding remarks

Providing a fully detailed account of the theorems in [4] proved quite daunting. In [4] P. Erdos and K. Mahler mention only briefly that corresponding results produced through their paper also hold for the numerator, however a proof is not provided. The gaps in [4] initially seemed small, however filling them in became quite difficult and complex. In order to show that the largest prime factor of the numerator increased rapidly with the convergents we needed an additional theorem – namely Theorem 3.5. Corollary 3.6 then immediately followed.

References

[1] Olds, C.D., *Continued Fractions*, Random House, Stanford, CA, 1963.

[2] Euler, Leonhard., *De fractionibus continuis dissertatio*, Commentarii academiae scientiarum Petropolitanae 9, pp. 98-137. 1744.

[3] Wiener, M.J., *Cryptanalysis of short RSA secret exponents*. IEEE Transactions on Information Theory. 36 (3): 553-558. 1990.

[4] Erdos, P., Mahler, K., *Some Arithmetical Properties Of The Convergents Of A Continued Fraction*, London Math. Soc. 12-18. 1939.

[5] Horek, J. *Method of continued fractions with application to atomic physics*, Physical Review A. 28 (4): 2151-2156. 1983.

[6] Sharaf, M. A., *Symbolic analytical developments of the zero pressure cosmological model of the universe*, Astrophysics & Space Science 318, no. 1/2: 133-140. 2008.

[7] R. Rivest, A. Shamir, and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM. 21 (2): 120-126. 1978.

[8] Diffie, W., and M. Hellman., *New directions in cryptography*, IEEE Transactions on Information Theory. 22 (6): 644-654. 1976.

[9] Lehmer, D. H., and R. E. Powers., *On factoring large numbers*, Bulletin of the American Mathematical Society. 37 (10): 770-777. 1931.

[10] Anderson, R.J., *A Practical RSA trapdoor*, Electronics Letters. 29 (11). 1993.

[11] B.S. Kaliski Jun., *Anderson's RSA Trapdoor Can Be Broken*, Electronics Letters, 29(15):1387-1388. 1993.

[12] Wallis, John., *Arithmetica infinitorum*, The Bavarian State Library. 1656.

[13] Elgamal, T., *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory. 31 (4): 469-472. 1985.

[14] Dirichlet, P.G.L., *Vorlesungen ber Zahlentheorie*, Vieweg. 1894.

[15] Nedashkovskiy N.A., and Kroshka T.I. *Solution of one class of nonlinear balance models of intersectoral ecological-economic interaction*, Cybernetics and Systems Analysis. 47 (5): 684-694. 2011.

[16] Bachmann, Paul., *Analytische Zahlentheorie*, Encyklopadie der mathematischen Wissenschaften. 1900.