

## THE PENTAGON

*A Mathematics Magazine for Students*

Volume 81 Number 2

Spring 2022

## Contents

<i>Kappa Mu Epsilon National Officers</i>	3
The VICCard Cipher: Our Contribution to the Field of Playing Card Cryptography <i>Isaac Reiter</i>	4
That's Impossible! An Exploration of Three Famous Impossibilities <i>Lisa Reed</i>	37
<i>The Problem Corner</i>	66
<i>Kappa Mu Epsilon News</i>	78
<i>Active Chapters of Kappa Mu Epsilon</i>	86

© 2022 by Kappa Mu Epsilon (<http://www.kappamuepsilon.org>). All rights reserved. General permission is granted to KME members for noncommercial reproduction in limited quantities of individual articles, in whole or in part, provided complete reference is given as to the source.

Typeset in WinEdt.

Printed in the United States of America.

*The Pentagon* (ISSN 0031-4870) is published semiannually in December and May by Kappa Mu Epsilon. No responsibility is assumed for opinions expressed by individual authors. Papers written by undergraduate mathematics students for undergraduate mathematics students are solicited. Papers written by graduate students or faculty will be considered on a space-available basis. Submissions should be made by means of an attachment to an e-mail sent to the editor. Either a TeX file or Word document is acceptable. An additional copy of the article as a pdf file is desirable. Standard notational conventions should be respected. Graphs, tables, or other materials taken from copyrighted works **MUST** be accompanied by an appropriate release form from the copyright holder permitting their further reproduction. Student authors should include the names and addresses of their faculty advisors. Contributors to The Problem Corner or Kappa Mu Epsilon News are invited to correspond directly with the appropriate Associate Editor.

---

**Editor:**

Doug Brown  
Department of Mathematics  
Catawba College  
2300 West Innes Street  
Salisbury, NC 28144-2441  
dkbrown@catawba.edu

**Associate Editors:**The Problem Corner:

Pat Costello  
Department of Math. and Statistics  
Eastern Kentucky University  
521 Lancaster Avenue  
Richmond, KY 40475-3102  
pat.costello@eku.edu

Kappa Mu Epsilon News:

Mark P. Hughes  
Department of Mathematics  
Frostburg State University  
Frostburg, MD 21532  
mhughes@frostburg.edu

---

*The Pentagon* is only available in electronic pdf format. Issues may be viewed and downloaded for **free** at the official KME website. Go to <http://www.pentagon.kappamuepsilon.org/> and follow the links.

## *Kappa Mu Epsilon National Officers*

Don Tosh

*President*

Department of Natural and Applied Sciences  
Evangel University  
Springfield, MO 65802  
toshd@evangel.edu

Scott Thuong

*President-Elect*

Department of Mathematics  
Pittsburg State University  
Pittsburg, KS 66762  
sthuong@pittstate.edu

Steven Shattuck

*Secretary*

School of Computer Science and Mathematics  
University of Central Missouri  
Warrensburg, MO 64093  
sshattuck@ucmo.edu

David Dempsey

*Treasurer*

Department of Mathematical, Computing, & Information Sciences  
Jacksonville State University  
Jacksonville, AL 36265  
ddempsey@jsu.edu

Mark P. Hughes

*Historian*

Department of Mathematics  
Frostburg State University  
Frostburg, MD 21532  
mhughes@frostburg.edu

John W. Snow

*Webmaster*

Department of Mathematics  
University of Mary Hardin-Baylor  
Belton, TX 76513

KME National Website:

<http://www.kappamuepsilon.org/>

# *The VICCard Cipher: Our Contribution to the Field of Playing Card Cryptography*

Isaac Reiter, *student*

PA Epsilon

Kutztown University  
Kutztown, PA 19530

## **Abstract**

Before computers, military tacticians and government agents had to rely on pencil-and-paper methods to encrypt information. For modern agents that want to use low-tech options in order to minimize their digital footprint, non-computerized ciphers are an essential component of their toolbox. Consider a deck of cards. There are  $52! \approx 2^{225.58}$  ways to mix a deck of cards. If each deck order is a key, this means that there are  $52! \approx 2^{225.58}$  different ways to encrypt a given message. To create some perspective, most computer ciphers feature either  $2^{128}$  or  $2^{256}$  different ways of encrypting the same message. Hence, a cipher created from a deck of cards has the potential to emulate the security of many computer ciphers. The focus of this paper is the creation of a unique, secure playing card cipher: VICCard. Its security is rooted in its combination of numerous cryptographic principles, including a substitution checkerboard, columnar transpositions, lagged Fibonacci generators, and junk letters. As evidenced by certain randomness tests, VICCard has the potential to extensively randomize an English plaintext.

## **Contents**

1 Introduction	5
1.1 Cryptography's Journey from Painting to PC	5
1.2 Why Playing Cards?	6
1.3 Existing Playing Card Ciphers	6
1.4 The Current Approach	7
2 VICCard	7
2.1 The Hollow Nickel Case	7
2.2 The First Version of VICCard	9
2.3 Step 1: Converting Letters to Cards	9
2.4 Step 2: Columnar Transpositions	11
2.5 Step 3: Lagged Fibonacci Generators	12
2.6 Step 4: Converting Cards Back into Letters	13
2.7 Summary: The Cards as a Key Container	14

3 Substitution Checkerboard	14
4 Columnar Transpositions	15
5 Lagged Fibonacci Generator	16
5.1 Modulo 4 Lagged Fibonacci Generator	16
5.2 Modulo 13 Lagged Fibonacci Generator	17
6 The Updated Version of VICCard	20
6.1 Plaintext Preparations	21
6.2 Triangular Columnar Transpositions	21
6.3 Junk Letters and Diffusion	23
7 Randomness Tests	27
7.1 Chi-Square Test on Ciphertexts	27
7.2 Chi-Square Test on One-Time Pads	29
7.3 The Washington Test	31
7.4 Interpreting the Results	31
8 Closing Thoughts	34
References	34

## 1 Introduction

### 1.1 Cryptography's Journey from Painting to PC

Cryptography is the science of safe, secure communication. It examines how to transform a message (called the plaintext) into an encoded form (called the ciphertext). An effective cryptologist must be proficient in two tasks: cryptography and cryptanalysis. Cryptography is the study of creating effective ciphers. Cryptanalysis is the study of breaking these ciphers. Cryptography is “code writing”, and cryptanalysis is “code breaking.” The creator of a secure cipher uses both of these skills. He first uses cryptography to create his cipher, and he then uses cryptanalysis to see whether his cipher is as secure as he thinks.

Egyptian hieroglyphics are one of the oldest instances of cryptography. For example, the tomb of Khnumhotep II featured a myriad of pictures and symbols. These pictographs told the story of the deceased with a beautiful visual display [10]. By contrast, cryptography is more frequently used for less aesthetic purposes: war and espionage.

Just as weapons of war have become more refined, cryptography has undergone careful attention and development. Humble ciphers such as Julius Caesar's cipher and the Vigenere cipher have given way to more advanced creations such as Rasterschlüssel 44 and VIC. As the ciphers became more complicated, they became more secure. However, they also became more impractical. As a result, cryptography's next step in its evolution was to enlist the help of machines. The most compelling example of this is the German Enigma machine. In order to break this cipher, the Allies enlisted cryptographers to fight fire with fire. To break the Enigma cipher they built an even better machine: a computer. Computer ciphers have now become the norm, encrypting everything from government secrets to emails between friends.

The advantage of computer ciphers is their ability to use formidable  $n$ -bit encryption. A cipher with  $n$ -bit encryption uses a pool of  $2^n$  possible keys, meaning that there are  $2^n$  possible ways of encrypting any given message. Typically, computer ciphers use 128-bit or 256-bit encryption. This prevents the ciphers from being cracked through brute force attempts that test every possible key.

Although cryptography has become mechanized since WWII, cryptographers have not discounted the strength and security of ciphers that are executed by hand. In fact, computerized ciphers can be based on the general cryptographic principles found in hand ciphers.

## 1.2 Why Playing Cards?

Here is an important observation. There are  $52!$  ways to permute a deck of cards. This means that there are  $52 \times 51 \times 50 \times 49 \times \dots \times 3 \times 2 \times 1$  ways to arrange a deck of cards. To give you an idea of the scope of this number, consider the following scenario that was adapted from a quote of Stephen Fry. Imagine a trillion universes, each of which contains a trillion planets. Each of these planets contains a trillion people, and each person has a trillion decks of cards. If everyone can shuffle all of their decks one time per second, it would take over two and a half trillion years before every possible deck order has been created [4]. Simply put, Fermilab estimates that there are approximately anywhere from  $10^{49}$  to  $10^{50}$  atoms that make up the earth [3]. This means that there are more ways to shuffle a deck of cards than there are atoms that compose the earth. Since  $52! \approx 2^{225.58}$ , a deck of cards has the potential to provide 225.58-bit encryption. This is enough to compete with the security provided by typical computer ciphers. From this arises the following question: can we use playing cards to create a secure, efficient hand cipher?

## 1.3 Existing Playing Card Ciphers

Given that the field of playing card ciphers is remarkably specialized, not a lot of playing card ciphers have been created. Aaron Toponce has a great website that lists most if not all of the publicly known playing card ciphers [16]. Before creating my own cipher, it was important to look at the work that has already been done. Performing cryptanalysis on existing ciphers can help determine both the strengths and weaknesses that tend to occur in playing cards ciphers. With this knowledge, one is better equipped to maximize the former and minimize the latter. Two playing card ciphers in particular are of interest.

First, Card-Chameleon is a playing card cipher created by Matthew McKague for his master's thesis [9]. His intention was to create a hand version of the computer algorithm RC4. At first glance, Card-Chameleon's straightforward, easy to remember algorithm makes it attractive. However, scrutiny of this cipher revealed a fatal weakness. Assuming a random key for each letter, Card-Chameleon encrypts any given letter into the exact same letter with probability  $\frac{1}{13}$ . Here's why this is a weakness. For each plaintext letter, the encryption algorithm should be such that every letter has the same probability of occurring. In other words, a plaintext letter should have a  $\frac{1}{26}$  probability of encrypting to any other letter. With

Card-Chameleon, however, it is disproportionately likely that a letter will encrypt to itself. Unfortunately, this deviation from the magic  $\frac{1}{26}$  probability is too significant to overlook (for more information, see the paper that Dr. Landquist and I wrote on this cipher [11]).

Second, Chaocipher is a cryptosystem that was created by John F. Byrne in 1918 [6]. Although Chaocipher has been around for over a century, the disclosure of the Chaocipher algorithm occurred as recently as 2010 [13]. As he was examining previously invented playing card ciphers, Toponce had the idea of adapting the Chaocipher algorithm to playing cards [15]. Given the respectable security of Chaocipher, I did not find a weakness that was as severe as that in Card-Chameleon. The closest thing to a weakness is the existence of plaintext/ciphertext pairs (or pt/ct pairs). A pt/ct pair is when two identical plaintext letters encrypt to the same ciphertext characters, such as two a's encrypting to two o's. Greg Mellen noticed that when he divided messages encrypted by Chaocipher into blocks of 13 letters, pt/ct pairs rarely occurred within these blocks [12]. Moshe Rubin hypothesized that pt/ct pairs will only occur if the two plaintext letters are separated by a distance of eight letters [12]. In order to put a rest to this question, I wrote a program that took two a's and tried every 1-letter, 2-letter, 3-letter, 4-letter, and 5-letter combination between these two a's. After testing all 12,356,630 of these cases, the program did not find any pt/ct pairs. However, it did find pt/ct pairs with certain 6-letter combinations. As a result, we can say for certain that at least six letters must be between two plaintext characters for a pt/ct pair to occur.

#### 1.4 The Current Approach

Analyzing existing ciphers revealed a general trend among them. Most if not all playing card ciphers are stream ciphers. This means that they encrypt plaintexts one letter at a time. The typical strategy is to first encrypt a letter and then alter the deck order before encrypting the next letter. In creating a unique cipher, I used a different approach. I focused my efforts on creating a block cipher. With a block cipher, the plaintext is encrypted in blocks of letters. Specifically with our cipher, we are encrypting the entire message at once in one large block.

## 2 VICCard

### 2.1 The Hollow Nickel Case

In 1953, Jimmy Bozart was a young 13-year-old boy living in Brooklyn. He delivered newspapers for the Brooklyn Eagle. On June 22, he was counting his tips when he noticed that one of his nickels was lighter than the others. As the nickel slipped from his fingers, it hit the floor and cracked neatly into two pieces. Inside, the nickel was completely hollow. Furthermore, it contained a tiny piece of microfilm with numbers on it [2].

When local police officers heard of this discovery, they scrambled to track down Jimmy and his nickel. Just in case he carelessly spent his valuable discovery,

they examined the Bingo money from the church and ice cream money from a Good Humor vendor. They eventually found Jimmy, who willingly gave them the nickel. Realizing the potential gravity of what they possessed, the New York police officers turned the coin over to the FBI [1].

In their research, the FBI investigators looked into whether the coin was simply a trick nickel meant for gags or magic tricks. This theory failed due to the imprecision with which the nickel was made. The hollow part was not big enough to contain much. Being a magician myself, I have handled high-quality hollow coins. The craftsman has to balance two factors. First, they have to make sure that the hollow coin is not too big. Otherwise, it will excite suspicion from the audience. On the other hand, the coin cannot be too small. If it is, anything that the magician is trying to hide inside the coin can easily get stuck. No feeling is worse than realizing mid-performance that your props are not cooperating. Jimmy's hollow nickel was not crafted with this much precision [2].

The FBI had to solve two questions: what was the coin's purpose, and what was the meaning of the numbers on the microfilm? In an exceptional stroke of luck, both questions were answered by Russian spy Reino Häyhänen. Häyhänen did not begin his espionage career by choice. Because he was fluent in Finnish, he was drafted as a translator for the Communist secret police during the Finnish-Soviet war. Upon the end of the war, he remained in Finland in order to report anti-Soviet individuals. Häyhänen became a member of the Communist party in 1943, and in 1948 the KGB assigned him a new task. Assuming the identity of Eugene Nicolai Maki, an immigrant from America to Estonia, he was to act as a Soviet spy in the United States. In 1957, Häyhänen contacted the U.S. embassy in Paris, desiring to defect to the United States. Following his defection, Häyhänen gave FBI officials the details of his operations. Most importantly, he revealed how hollow coins, such as the one found by Jimmy, were used to exchange information. Soviet agents agreed on inconspicuous locations called "dead drops" in which they placed secret containers such as hollow coins [2].

The only remaining piece of the puzzle was to decrypt the message that was inside the coin. Häyhänen thoroughly explained the cipher that was used to encrypt the message on the microfilm inside the nickel [2]. It was encrypted using a Nihilist cipher called VIC [17]. The Nihilists were a Russian group that opposed the Russian tsar. In the 1880s, the Nihilists used ciphers in order to communicate, which became known as the Nihilist ciphers [5]. In a bizarre twist of fate, the message in the nickel was actually intended for Häyhänen himself. After he accidentally spent the nickel, it traveled from person to person until it eventually landed into Jimmy's inquisitive hands [1].

The CIA has an excellent description of how VIC works [7]. Häyhänen presented this description at the 1957 trial of Colonel Rudolf Abel. Since the CIA states that those attending the trial were either bored or confused by the description of VIC, I will spare you the details. Instead, I will describe the specific aspects of VIC that provided the inspiration for VICCard.

## 2.2 The First Version of VICCard

To pay homage to the mind-numbing security of VIC, I have decided to entitle my original cipher VICCard. VICCard is an original playing card cipher that combines numerous cryptographic strategies together. The basic strategy of VIC is to use a checkerboard to convert letters to cards and then to perform various operations on these cards. With VICCard, we are using a similar strategy. There are four steps to this cipher. First, use a checkerboard to convert the letters of the message into cards. Second, perform columnar transpositions on these cards. Third, apply lagged Fibonacci generators to these cards. Finally, use the same checkerboard to convert the cards back into letters. Although VICCard has gone through multiple versions, these four steps remained the fundamental structure. In order to demonstrate each of these steps, we will follow cryptographic tradition and encrypt the message *Attack At Dawn* as an example. The following deck of cards will be our key. In our notation,  $9\heartsuit$  is the top card and  $A\heartsuit$  is the bottom card when the deck is held face up.

[ $A\heartsuit, 7\heartsuit, K\clubsuit, 8\heartsuit, K\diamondsuit, J\clubsuit, K\spadesuit, K\heartsuit, 4\spadesuit, 8\diamondsuit, 4\heartsuit, 7\clubsuit, 3\clubsuit, 10\diamondsuit, Q\heartsuit, 10\clubsuit, 5\diamondsuit, 2\spadesuit, J\spadesuit, A\clubsuit, 9\clubsuit, 4\clubsuit, 3\diamondsuit, 3\heartsuit, 8\clubsuit, 7\diamondsuit, 5\spadesuit, 5\heartsuit, 2\clubsuit, A\diamondsuit, 8\spadesuit, 10\spadesuit, 6\heartsuit, 9\spadesuit, 10\heartsuit, 6\diamondsuit, Q\diamondsuit, 6\clubsuit, 2\diamondsuit, J\diamondsuit, 7\spadesuit, 5\clubsuit, 4\diamondsuit, J\heartsuit, Q\spadesuit, 6\spadesuit, 3\spadesuit, Q\clubsuit, 9\heartsuit, 2\heartsuit, A\spadesuit, 9\diamondsuit$ ]

## 2.3 Step 1: Converting Letters to Cards

We will have cards represent letters according to the following table. Notice that the lowercase letters are represented by the black cards and that the uppercase letters are represented by the red cards.

	Spades (♠)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	a	b	c	d	e	f	g	h	i	j	k	l	m
	Clubs (♣)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	n	o	p	q	r	s	t	u	v	w	x	y	z
	Hearts (♥)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
	Diamonds (♦)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 1: Letter encoding for VICCard

In order to convert the letters of the plaintext into cards, we will use a checkerboard. The checkerboard in Table 2 is created by dealing the cards into 4 columns of 13 cards.

	♣ (0)	♥ (1)	♠ (2)	♦ (3)
A (1)	A♥	10♦	5♠	J♦
2 (2)	7♥	Q♥	5♥	7♠
3 (3)	K♣	10♣	2♣	5♣
4 (4)	8♥	5♦	A♦	4♦
5 (5)	K♦	2♠	8♠	J♥
6 (6)	J♣	J♠	10♠	Q♠
7 (7)	K♠	A♣	6♥	6♠
8 (8)	K♥	9♣	9♠	3♠
9 (9)	4♠	4♣	10♥	Q♣
10 (10)	8♦	3♦	6♦	9♥
J (11)	4♥	3♥	Q♦	2♥
Q (12)	7♣	8♣	6♣	A♠
K (0)	3♣	7♦	2♦	9♦

Table 2: Checkerboard from Deck Order

Suppose that we are encrypting the plaintext **Attack At Dawn**. We will convert these letters to cards one letter at a time. We will start with the letter **A**, which is represented by **A♥**. First, I find **A♥** in the checkerboard. This card is in the **A** row and the **♣** column. Hence, **A** encrypts to **A♣**. Next, we move onto the letter **t**, which is represented by **7♣**. This card is in the **Q** row and the **♣** column. Hence, **t** encrypts to **Q♣**. Continuing this pattern, the plaintext **Attack At Dawn** is converted to **A♣, Q♣, Q♣, Q♦, 8♦, 6♥, A♣, Q♣, J♣, Q♦, 3♥, 7♥**.

A	t	t	a	c	k	A	t	D	a	w	n
A♣	Q♣	Q♣	Q♦	8♦	6♥	A♣	Q♣	J♣	Q♦	3♥	7♥
1	12	12	12	8	6	1	12	11	12	3	7
0	0	0	3	3	1	0	0	0	3	1	1

Table 3: Letters Converted to Face Values and Suits

Typically with effective cryptographic checkerboards, each plaintext letter is represented by 2 or more numbers. Instead of using this string of cards, we will break up the cards into two rows. The first row is all of the face values of the cards, and the second row is all of the suits. The face values are represented with the numbers 0 through 12, and the suits are represented with the numbers 0 through 3.

At this point, it is important to take notice of a security feature of this checkerboard. Notice that every letter is represented by a black card and a red card. The black card represents the lowercase version, and the red card represents the uppercase version. In the above example, I used the black cards to represent each lowercase letter and the red cards to represent each uppercase letter. However, I did not have to do this. For each plaintext letter, we can either use the black card or the red card to encrypt it. For example, instead of using **A♥** for the letter **A**, we can instead use the black card option **A♠**. This is equivalent to regularly encrypting the letter **a**. Similarly, instead of encrypting **t** as **Q♣**, we can encrypt it as **Q♦**.

This is exactly like regularly encrypting the letter T. In other words, the option of choosing either the black card or the red card for each letter is equivalent to the option of changing the case of each letter. For example, based on how we choose black and red cards, we can encrypt the message Attack At Dawn as aTtacK AT daWN. When the decoder reverses this process, he will get the latter plaintext message. The letters are in the wrong cases, but it is still readable. Hence, having this choice for each letter does not compromise the message.

This feature has great potential for increasing security. Suppose that we have a plaintext of  $N$  letters. Since there are two choices for each letter, a black card or a red card, the encoder has  $2^N$  possible ways of using the same deck to encrypt a particular message. Recall that there are about  $2^{225.58}$  possible decks. Combining these two together, there are  $2^{225.58+N}$  possible ways of encrypting the same message. In other words, every letter in the plaintext adds a bit to the pool of possible keys.

## 2.4 Step 2: Columnar Transpositions

In Step 1, we performed a substitution: cards were substituted for letters. In Step 2, we will perform a transposition. Here, none of the numbers are going to be altered. Instead, they are going to be rearranged via a columnar transposition. We will use two columnar transpositions: one for the row of face values and one for the row of suits. Here is how we perform columnar transpositions. First, we need a key for each transposition. We will use the order of the clubs for the face values:

$[K\clubsuit, J\clubsuit, 7\clubsuit, 3\clubsuit, 10\clubsuit, A\clubsuit, 9\clubsuit, 4\clubsuit, 8\clubsuit, 2\clubsuit, 6\clubsuit, 5\clubsuit, Q\clubsuit]$ .

Also, we will use the order of the hearts excluding the king for the suits:

$[A\heartsuit, 7\heartsuit, 8\heartsuit, 4\heartsuit, Q\heartsuit, 3\heartsuit, 5\heartsuit, 6\heartsuit, 10\heartsuit, J\heartsuit, 9\heartsuit, 2\heartsuit]$ .

To transpose the face values, we create a grid with the clubs on top. Then, we fill in the grid from left to right with the face values.

$K\clubsuit$	$J\clubsuit$	$7\clubsuit$	$3\clubsuit$	$10\clubsuit$	$A\clubsuit$	$9\clubsuit$	$4\clubsuit$	$8\clubsuit$	$2\clubsuit$	$6\clubsuit$	$5\clubsuit$	$Q\clubsuit$
1	12	12	12	8	6	1	12	11	12	3	7	

Next, we read the face values out of the grid from top to bottom based on the numerical order of the clubs. We first read 6 from the  $A\clubsuit$  column, 12 from the  $2\clubsuit$  column, 12 from the  $3\clubsuit$  column, and so forth to get the following new row of face values: (6 12 12 12 7 3 12 11 1 8 12 1). Similarly, to perform the transposition of the suits we create a grid with the hearts on top. Then, we again fill in the grid from left to right.

$A\heartsuit$	$7\heartsuit$	$8\heartsuit$	$4\heartsuit$	$Q\heartsuit$	$3\heartsuit$	$5\heartsuit$	$6\heartsuit$	$10\heartsuit$	$J\heartsuit$	$9\heartsuit$	$2\heartsuit$
0	0	0	3	3	1	0	0	0	3	1	1

Reading out the suits from the top to bottom based on the numerical order of the suits, we get the following new row of suits: (0 1 1 3 0 0 0 0 1 0 3 3). In summary,

performing these columnar transpositions gives us the following two new rows of face values and suits:

6	12	12	12	7	3	12	11	1	8	12	1
0	1	1	3	0	0	0	0	1	0	3	3

### 2.5 Step 3: Lagged Fibonacci Generators

The third step of VICCard is to use two lagged Fibonacci generators. Frequently in cryptography, we employ the help of random strings of numbers. However, the problem with using humongous strings of random numbers is that they are wildly impractical. Instead, it is more common to use pseudorandom strings of numbers. These are strings of numbers that appear to be random and have a lot of the properties of randomness, even though they were not created in a purely random way.

A lagged Fibonacci generator is one such method of creating a pseudorandom string of numbers. Instead of sharing the entire string of numbers, the sender and receiver only share a small string of a few digits. This is called the seed. For example, suppose that we are using the first five digits of  $\pi$  as the seed: (3 1 4 1 5). Here is the procedure for creating an indefinitely long string of numbers by using a lagged Fibonacci generator. We begin with the first two numbers: 3 and 1. We add these together to get 4, and we attach this number to the end of the seed: (3 1 4 1 5 4). Next, we move onto the next two numbers: 1 and 4. Adding these together gives us 5, which we attach to the end of the previous string of numbers: (3 1 4 1 5 4 5). Again, we add the next two numbers (4 and 1) to get 5, which is again attached to the end: (3 1 4 1 5 4 5 5). Continuing this process indefinitely, we can create a pseudorandom string of numbers of any desired length. Also, it is important to note that this addition is performed modulo 10. This means that if adding two numbers produces a number that is greater than 10, we divide this number by ten and use the remainder. For example, adding 5 and 7 gives us 12, which is 2 in modulo 10.

The convenience of a lagged Fibonacci generator is rooted in the fact that the sender and receiver only need to share the seed. In order to do this with VICCard, we will encode two seeds in the deck. The seed for the lagged Fibonacci generator of the face values is encoded in the order of the spades in the deck. The order of the spades in the current keyed deck is

$[K\spadesuit, 4\spadesuit, 2\spadesuit, J\spadesuit, 5\spadesuit, 8\spadesuit, 10\spadesuit, 9\spadesuit, 7\spadesuit, Q\spadesuit, 6\spadesuit, 3\spadesuit, A\spadesuit]$ .

The order of the face values of these cards yields the following seed: (13 4 2 11 5 8 10 9 7 12 6 3 1). As one more adjustment, we will represent the 13, which came from  $K\spadesuit$ , as  $13 \bmod 13 = 0$ . Hence, the seed for the lagged Fibonacci generator of the face values is (0 4 2 11 5 8 10 9 7 12 6 3 1).

Similarly, the seed for the lagged Fibonacci generator of the suits is encoded in the order of the face values of the diamonds. The order of the diamonds in the current keyed deck is

$[K\diamond, 8\diamond, 10\diamond, 5\diamond, 3\diamond, 7\diamond, A\diamond, 6\diamond, Q\diamond, 2\diamond, J\diamond, 4\diamond, 9\diamond]$ .

This gives us the following seed: (13 8 10 5 3 7 1 6 12 2 11 4 9). Since there are only four suits in a deck, we will express this seed in modulo 4. Hence, the seed for the lagged Fibonacci generator of the suits is (1 0 2 1 3 3 1 2 0 2 3 0 1).

We will now add these two string of numbers to the rows of face values and suits using modulo 13 and modulo 4 arithmetic, respectively. In this case, the plaintext is small enough so that we do not have to generate any more numbers. If the plaintext were longer, we would use each seed to create new numbers as detailed above. Adding the numbers from the spade lagged Fibonacci generator to the row of face values, we get the following:

	6	12	12	12	7	3	12	11	1	8	12	1
+	0	4	2	11	5	8	10	9	7	12	6	3
=	6	3	1	10	12	11	9	7	8	7	5	4

Adding the numbers from the diamond lagged Fibonacci generator to the row of suits, we get the following:

	0	1	1	3	0	0	0	0	1	0	3	3
+	1	0	2	1	3	3	1	2	0	2	3	0
=	1	1	3	0	3	3	1	2	1	2	2	3

This has the effect of continuing to randomize the face values and suits independently. In total, this gives us the following two new rows of face values and suits:

6	3	1	10	12	11	9	7	8	7	5	4
1	1	3	0	3	3	1	2	1	2	2	3

## 2.6 Step 4: Converting Cards Back into Letters

The final step in the VICCard cipher is to convert these two rows of numbers back into letters. In order to do this, we will use Table 2 and reverse the algorithm of Step 1. We will start with the first column of numbers, which contains a face value of 6 and a suit of 1 ( $\heartsuit$ ). This tells us to look at the card in the sixth row and the  $\heartsuit$ 's column of the checkerboard, which is  $J\spadesuit$ . Since  $J\spadesuit$  represents the letter k, the first letter of the ciphertext is k. Next, the second column of numbers tells us to look at the card in the third row and the  $\heartsuit$ 's column, which is  $10\clubsuit$ . This card represents the letter w, meaning that the next letter of the ciphertext is w. Continuing this pattern, we get the following ciphertext: kwXUaB qF vFhQ.

## 2.7 Summary: The Cards as a Key Container

Something that you might have noticed about VICCard is that playing cards are technically not needed to perform it. Substitution checkerboards, columnar transpositions, and lagged Fibonacci generators are not unique to playing cards. In fact, this cipher can be entirely executed using numbers instead of face values and suits. However, suppose that we do not use playing cards to execute VICCard. Here, the one sending the message and the one receiving the message must share a remarkable amount of information. They must both know the order of letters in the checkerboard, the keywords used for the transpositions, and the seeds for the lagged Fibonacci generators. The reason for executing this cipher with playing cards is because all of this information is compactly contained in 52 playing cards. This way, the sender and receiver must only share the deck order.

Now that we have used cryptography to create VICCard, the next step is to use cryptanalysis to analyze its security. We will examine each element of VICCard: the substitution checkerboard, the columnar transpositions, and the lagged Fibonacci generators.

## 3 Substitution Checkerboard

Basic cryptographic substitutions can be found in cryptogram puzzle books. In these books, every English letter is represented by another letter. For example, every e is replaced with w and every x is replaced by c. There are  $26! \approx 4.03 \times 10^{26}$  possible ways to substitute each English letter for another English letter. At first glance, it seems that a standard cryptogram is remarkably secure. However, if that were true, cryptogram books would not be available in giant puzzle books alongside Sudoku and crosswords. The insecurity of cryptograms is best exemplified by two common cryptanalysis methods. First, analyzing the frequency distribution of English letters is a useful technique of decoding a cryptogram. For example, e is the most common English letter. Since e encrypts to w in the above example, it is likely that w will be the most common letter in the ciphertext. Hence, a code breaker could deduce from the high frequency of w that it represents e. A second attack is the use of plaintext cribs. Whereas the first attack exploits the frequencies of certain letters, cribs are frequently occurring words. For example, if I see a letter by itself in the ciphertext, it is likely that it represents the letter a. Similarly, if I see a three letter word in the ciphertext, it is likely that this is either the word the or a pronoun. Hence, there is a high chance that I can ascertain the identities of three letters.

Instead of a basic one-to-one substitution, a more secure method is to represent each plaintext character by two or more characters. This technique is known as fractionation, and it is present in ciphers such as Bifid, Trifid, and straddling checkerboard [18]. With Bifid, each English letter is represented by two numbers. We substitute each letter in the plaintext with two numbers and shuffle these numbers around. Then, we substitute each pair of numbers in the final sequence for their English letter equivalents. Trifid substitutes three numbers for each English

letter, and a straddling checkerboard encrypts some letters with one number and some letters with two numbers.

The substitution checkerboard in VICCard follows an approach that is similar to Bifid. Each letter is substituted for two numbers; one number represents a face value, and the other number represents a suit. However, an important difference is the ability of VICCard to perform two different substitutions for each letter. We can either use the corresponding red uppercase card or the corresponding black lowercase card. With Bifid and similar substitution checkerboards, we always encrypt a letter with the same group of numbers. Here, VICCard can encrypt the exact same letter in two different ways. This is especially useful when messages use the same letter numerous times throughout the message (such as the a's in Attack At Dawn) or when words contain two of the same letter that are next to each other (such as the two t's in Attack). In Bifid, a code breaker has a  $\frac{1}{26}$  probability of correctly guessing the letter represented by the two numbers. In VICCard, the code breaker has to guess the two cards that represent the same letter, which he has a  $\frac{1}{26} \times \frac{1}{26} = \frac{1}{676}$  probability of doing correctly. This further complicates the code breaker's task without severely complicating the encryption process.

#### 4 Columnar Transpositions

On its own, the double columnar transposition is an alluring cipher: it is easy to learn, fast to implement, and not so trivial to break. In attempting to successfully break this cipher, the first option that comes to mind is simply testing every possible keyword [8]. For a nine column transposition, there are  $9! = 362,880$  possible keys. A computer can quickly move through each of these keys, easily cracking the cipher. This is why columnar transpositions are typically performed in pairs. There are  $(9!)^2 = 131,681,894,400$  possible permutations with a pair of nine column transpositions. A second possible attack is a dictionary attack [8]. Here, the code breaker has a database of about 1 million frequently used keywords, such as names of prominent historical figures. He then tests each keyword to see whether it successfully decodes the message. Yet a third strategy is hill climbing [8]. This involves picking a starting keyword and gradually making small changes to this keyword, such as swapping letters. If the new keyword seems to decode the message better, then this keyword replaces the starting one. With hill climbing, we continue to make these changes until we find the keyword.

A vital feature of all these strategies is that keywords are guessed until the ciphertext is undone in such a way that it "makes sense." This is why transpositions are frequently combined with substitutions. Consider when the letters in a plaintext message are substituted in some way for others. After this, the two columnar transpositions are performed. This complicates these common code-breaking techniques because now it is impossible for any reversal of the transpositions to "make sense." This is why VICCard combines substitutions with transpositions. In fact, VICCard uses three substitutions: initially converting letters to cards, applying lagged Fibonacci generators, and finally converting cards back into letters.

Hence, the double columnar transposition in VICCard is valuable in and of itself. However, it becomes remarkably strong when combined with the other cryptographic techniques.

## 5 Lagged Fibonacci Generator

In assessing the security of a lagged Fibonacci generator, two features must be analyzed. First, what is the period? In other words, how many numbers does the lagged Fibonacci generator create before it starts repeating? In emulating true randomness, we do not want a string of numbers that repeats. Hence, we desire a lagged Fibonacci generator with a large period. Specifically, the security of a lagged Fibonacci generator is maximized when its period is larger than the length of the plaintext. Second, does the distribution of the numbers closely resemble the distribution produced by randomness? For example, there are four different numbers in the lagged Fibonacci generator of the suits. In a truly random string of 4 different numbers, each number occurs approximately  $\frac{1}{4}$  of the time. Hence, this lagged Fibonacci generator resembles a random distribution if the 0's, 1's, 2's, and 3's all occur approximately  $\frac{1}{4}$  of the time.

### 5.1 Modulo 4 Lagged Fibonacci Generator

In analyzing the security of the modulo 4 lagged Fibonacci generator, the seed of which is the order of the diamonds, I first created all the possible seeds. These periods each have three 0's, three 2's, three 4's, and four 1's. Hence, there are  $\binom{13}{3} \binom{10}{3} \binom{7}{3} = 1,201,200$  seeds to consider. As a result, it was necessary to write a program that created each of these seeds and placed them into text files. After this, I created a program in order to ascertain the period of each seed. It did this by reading each seed in from the text files, used each seed to create a string of about 100,000 numbers, and searched the string of numbers to see when the string began to repeat. Analyzing all the seeds in this way, it became clear that there are three possible periods. 23 seeds have a period of 62, 1019 seeds have a period of 510, and the remaining 1,200,158 seeds have a period of 15,810. Overall, this is very good news:  $\frac{1,200,158}{1,201,200} \approx 99.9\%$  of the seeds have a respectable period of 15,810. 15,810 characters can fill almost eight pages of a Word document in MLA format, assuming that there are no spaces. This is more than what is needed to send a typical encoded message.

Once I knew the period of each seed, I then determined the distribution of 0's, 1's, 2's, and 3's produced by each seed. I accomplished this by writing a program which used each seed to produce a string of numbers until right before it started repeating. In other words, the program produced strings of 62 numbers from the seeds that have a period of 62, produced strings of 510 numbers from the seeds that have a period of 510, and so forth. It then went through each string of numbers and counted the number of occurrences of 0's, 1's, 2's, and 3's. On average, each seed created a distribution that very closely approximated 25% of 0's, 1's, 2's, and 3's. Table 4 shows the average number of 0's, 1's, 2's, and 3's for each period.

Seeds with a period of 62			
Number of 0's	Number of 1's	Number of 2's	Number of 3's
15.3913	16.8696	14.6087	15.1304
Seeds with a period of 510			
Number of 0's	Number of 1's	Number of 2's	Number of 3's
127.421	128.495	126.579	127.505
Seeds with a period of 15,810			
Number of 0's	Number of 1's	Number of 2's	Number of 3's
3952.47	3953.32	3951.8	3952.4

Table 4: Average Distribution for the Modulo 4 lagged Fibonacci generator

Table 5 shows the percent error of each average relative to 25% of the period. As the period increases, the percent error decreases.

Seeds with a period of 62			
Percent Error of 0's	Percent Error of 1's	Percent Error of 2's	Percent Error of 3's
-0.7%	8.8%	-5.8%	-2.4%
Seeds with a period of 510			
Percent Error of 0's	Percent Error of 1's	Percent Error of 2's	Percent Error of 3's
-0.06196%	0.7804%	-0.7224%	0.003922%
Seeds with a period of 15,810			
Percent Error of 0's	Percent Error of 1's	Percent Error of 2's	Percent Error of 3's
$-7.590 \times 10^{-4}\%$	$2.075 \times 10^{-2}\%$	$-1.771 \times 10^{-2}\%$	$-2.530 \times 10^{-3}\%$

Table 5: Percent Errors of the Distribution for the Modulo 4 lagged Fibonacci generator

## 5.2 Modulo 13 Lagged Fibonacci Generator

In order to analyze the security of the modulo 13 lagged Fibonacci generator, which is encoded in the order of the spades, I followed a similar process. I first examined the periods and then analyzed the distributions. Before any of this could be done, however, I had to determine which seeds to test. There are  $13! = 6,227,020,800$  possible seeds, making it impractical to test all of them. Instead, I chose a random sampling of seeds to test. Specifically, I analyzed all the seeds that start with (8 4 12 5), all the seeds that start with (12 6 9 8), all the seeds that start with (1 9 12 7), all the seeds that start with (3 2 11 7), and all the seeds that start with (3 1 5 2). There are  $9! = 362,880$  seeds in each of these categories, meaning that I analyzed  $5 \times 362,880 = 1,814,400$  seeds. Of course, before testing any of these seeds, I had to create five text files containing each of these categories of seeds. I did this by creating a program that created every possible permutation of any number of objects. Since the seed contains 13 numbers, I used the 13 setting of my program. Furthermore, I filled in the first four numbers for each category (like 8 4 12 5). This program then created every possible permutation of the nine remaining numbers and wrote all the seeds to a text file with the appropriate label. For example, the program wrote all seeds beginning with (8 4 12 5) to a file entitled "EightFourTwelveFive.txt." Once I compiled this respectable sample size, I began testing each seed.

Recall that most of the seeds of the modulo 4 lagged Fibonacci generator have a period of 15,810. We are not as concerned with the exact periods of the modulo 13 seeds. As long as the periods of the latter are larger than those of the former, then the periods of the modulo 13 seeds are secure for our current purposes. In order to test this, I created a program that took each seed in the previously created files, used each to create a string of slightly more than 15,810 numbers, and searched the string to see if the pattern repeated. Of all the 1,814,400 seeds that were tested, none of them repeated within 15,810 numbers. Just out of curiosity, I took a random seed (8 4 12 5 0 7 9 10 2 3 1 11 6) and tried to determine its period. After creating a string of 3,000,000 numbers, the pattern of numbers still did not repeat. As a result, we can conclude that the modulo 13 lagged Fibonacci generator has a respectable, secure period.

Next, I needed to make sure that the lagged Fibonacci generator produces a uniform distribution of the numbers 0 through 12. In order to do this, I created yet another program that used each seed to create a string of 13,000 numbers. It then counted the number of occurrences of each number in each string. Tables 6 through 11 show the average results for each of the five groups of seeds and the overall average for all 1,814,400 seeds.

Seeds That Begin with 8 4 12 5	
Number	Average Number of Occurrences
0	1003.31
1	998.494
2	1003.03
3	999.091
4	1001.6
5	998.142
6	998.786
7	1001.39
8	998.25
9	998.963
10	999.007
11	1000.6
12	999.329

Table 6: Average Distribution for Modulo 13 Lagged Fibonacci Generator (8 4 12 5)

Seeds That Begin with 12 6 9 8	
Number	Average Number of Occurrences
0	999.686
1	999.94
2	998.537
3	1001.64
4	1000.73
5	999.861
6	1001.15
7	1000.81
8	999.764
9	1000.17
10	999.243
11	997.879
12	1000.6

Table 7: Average Distribution for Modulo 13 Lagged Fibonacci Generator (12 6 9 8)

Seeds That Begin with 1 9 12 7	
Number	Average Number of Occurrences
0	1002.66
1	999.659
2	999.788
3	999.473
4	1003.42
5	999.352
6	999.374
7	997.423
8	1000.33
9	998.763
10	999.384
11	1001.46
12	998.911

Table 8: Average Distribution for Modulo 13 Lagged Fibonacci Generator (1 9 12 7)

Seeds That Begin with 3 2 11 7	
Number	Average Number of Occurrences
0	1000.46
1	997.528
2	1000.79
3	999.103
4	999.776
5	1004.38
6	998.065
7	1001.08
8	999.167
9	1001.5
10	999.008
11	1000.48
12	998.668

Table 9: Average Distribution for Modulo 13 Lagged Fibonacci Generator (3 2 11 7)

Seeds That Begin with 3 1 5 2		
Number	Average Number of Occurrences	
0	1000.46	
1	998.955	
2	1000.42	
3	998.035	
4	1001.65	
5	998.509	
6	1000.09	
7	1003.48	
8	1001.21	
9	998.733	
10	999.764	
11	997.494	
12	1001.19	

Table 10: Average Distribution for Modulo 13 Lagged Fibonacci Generator (3 1 5 2)

Results for all 1,814,400 Seeds			
Number	Average Number of Occurrences		Percent Error
0	1001.3152		0.13152%
1	998.9152		-0.10848%
2	1000.513		0.0513%
3	999.4684		-0.05316%
4	1001.4352		0.14352%
5	1000.0488		0.00488%
6	999.493		-0.0507%
7	1000.8366		0.08366%
8	999.7442		-0.02558%
9	999.6258		-0.03742%
10	999.2812		-0.07188%
11	999.5826		-0.04174%
12	999.7396		-0.02604%

Table 11: Average Distribution for Modulo 13 Lagged Fibonacci Generator Overall

If these strings of 13,000 numbers were truly random, we would expect approximately 1000 of each number. As demonstrated by these tables, the lagged Fibonacci generator in question provides an incredible approximation of this distribution. As a result, we can conclude that the modulo 13 lagged Fibonacci generator is safe to use.

## 6 The Updated Version of VICCard

The above description of VICCard is the first version of the cipher that was used to outline the basic structure. It is composed of the following basic steps:

1. Convert the plaintext letters to cards using the checkerboard.
2. Perform one columnar transposition on both the face value row and the suit row.
3. Add one pseudorandom string of numbers to both the face value row and the suit row.

4. Use the same checkerboard in Step 1 to convert the cards back into letters.

In an attempt to make improvements, VICCard has gone through multiple versions. This basic four-step structure remains the same throughout each update. The following details the fifth version of the cipher, VICCard 5.0, which is the most recent update. This version uses three additional cryptographic strategies.

### 6.1 Plaintext Preparations

First, I added two small options to prepare the plaintext before encryption. First, I added the option of placing junk letters at both the beginning and the end of the message. Second, the encoder can “cut” the message before encrypting it. This is similar to cutting a deck of cards. In order to mark where he cuts the cards, he should place a marker, such as xx, where the intelligible words begin. Let’s apply these two strategies to encrypting Attack At Dawn. First, we add random characters to the beginning and the end to get

EdfFxxAttackAtDawnsjfsDRmk.

Second, we will “cut” the message at the k in Attack, giving us

kAtDawnsjfsDRmkEdfFxxAttac.

Now, we can move on to the four steps of VICCard 5.0 to encrypt the message. When the decoder decrypts the ciphertext, he will get

kAtDawnsjfsDRmkEdfFxxAttac

as his message. In order to read it, all he needs to do is “cut” the marker xx to the end:

AttackAtDawnsjfsDRmkEdfFxx.

Removing the junk letters at the end, he can now read the message:

AttackAtDawn dsjfsDRmkEdfFxx.

### 6.2 Triangular Columnar Transpositions

In the first version of VICCard, exactly one columnar transposition is performed on the face values and the suits. However, to increase security, columnar transpositions are typically performed in pairs. Hence, the current version of VICCard applies double columnar transpositions to the face values and to the suits. This is a total of four columnar transpositions. Thus, we will use the following four keys. For the face values, the orders of A♣ through 7♣ and of A♥ through 6♥ shall be the keys for the first and second transpositions, respectively. For the suits, the orders of 7♥ through K♥ and of 8♣ through K♣ shall be the keys for the first and second transpositions, respectively.

Furthermore, following the pattern of VIC, we shall make the second transposition a little different. For the second transposition, the VIC cipher reads numbers out of the grid in exactly the same way: from the top to the bottom based on the keyword. However, VIC places numbers into the grid differently.

For example, we will use the following order of six hearts to perform a face value transposition: [5♥, 6♥, 3♥, A♥, 2♥, 4♥]. Before filling the transposition grid, we will use the key to divide the grid into triangular sections. We will represent these sections by filling them with the letter T. We will start with the smallest number of the key, which is 1. We section off all cells to the right of and

including the part of the grid under the 1. We repeat this process on the next row, starting at the next column over. We continue to section off cells until we run out of columns, producing a triangular pattern.

We do this for all numbers in the key. The following grid shows the results of sectioning off cells based on the numbers 1-4.

5	6	3	1	2	4
			T	T	T
				T	T
					T
				T	T
					T
		T	T	T	T
			T	T	T
				T	T
					T
					T

We will transpose the following sequence of face values: (4 0 8 12 5 1 6 8 9 0 1 9 1 8 7 11 12 8 9 6 3 2 2 12 7 0 12 7). Since there are 28 face values, we know that we will completely fill four rows and partially fill a fifth row. With this in mind, we begin by filling in all the cells that have not been sectioned off.

5	6	3	1	2	4
4	0	8	T	T	T
12	5	1	6	T	T
8	9	0	1	9	T
1	8	7	11	T	T
12	8	9	6		T

Now, we place the rest of the face values in the sectioned off cells.

5	6	3	1	2	4
4	0	8	3	2	2
12	5	1	6	12	7
8	9	0	1	9	0
1	8	7	11	12	7
12	8	9	6		

Finally, we finish the transposition by reading the numbers out from the grid: (3 6 1 11 6 2 12 9 12 8 1 0 7 9 2 7 0 7 4 12 8 1 12 0 5 9 8 8).

This unique transposition contributed to the remarkable security of VIC. As a result, it makes sense to apply it to VICCard. With VICCard 5.0, the first transposition for the face values and the suits is a normal columnar transposition. By contrast, the second transposition for the face values and the suits is this special transposition.

### 6.3 Junk Letters and Diffusion

Finally, these last two cryptographic strategies are performed before each columnar transposition. First, VICCard 5.0 adds random face values and suits during the columnar transpositions. For example, we will work with the following rows of face values and suits:

1	12	12	12	8	6	1	12	11	12	3	7
0	0	0	3	3	1	0	0	0	3	1	1

Consider the face values. We will perform the following columnar transposition with seven columns:

7	3	1	4	2	6	5
1	12	12	12	8	6	1
12	11	12	3	7		

Notice that the bottom row is partially filled. In the first version of VICCard, we performed the transposition with this partially filled row. In VICCard 5.0, we fill this bottom row with junk face values before completing the transposition. If the bottom row is completely filled, we will add an entire row of junk face values.

7	3	1	4	2	6	5
1	12	12	12	8	6	1
12	11	12	3	7	5	9

Now, we perform the columnar transposition: (12 12 8 7 12 11 12 3 1 9 6 5 1 12). Next, we will add four random face values to make the total number divisible by 6: (12 12 8 7 12 11 12 3 1 9 6 5 1 12 2 5 6 3). We then execute a special triangular columnar transposition with six columns:

1	4	3	5	6	2
7	12	11	12	3	1
12	9	6	5	1	12
12	8	2	5	6	3

These two transpositions produce the following string of face values: (7 12 12 1 12 3 11 6 2 12 9 8 12 5 5 3 1 6).

Notice that during the transpositions, the random numbers are spread throughout the stream of face values. When the decoder is undoing the transpositions, the random characters are easily eliminated. For example, undoing the above transposition produces the following stream of numbers: (12 12 8 7 12 11 12 3 1 9 6 5 1 12 2 5 6 3). Currently, the random characters are at the end of the message. However, the decoder still needs to determine how many random characters there are. All they have to do is divide the string of numbers into sections of seven numbers and eliminate what remains: (12 12 8 7 12 11 12 | 3 1 9 6 5 1 12 | 2 5 6 3). The reason for this is that the first columnar transposition produces a string

of numbers that is divisible by 7. Since the second columnar transposition adds anywhere from 1 to 6 more numbers, all the leftover numbers must be junk letters.

Second, the last new security feature is a method of creating diffusion. Diffusion refers to when a given plaintext letter has an effect on how other plaintext letters are encrypted. Suppose that I am going to perform a seven-column transposition with the following string of face values: (12 5 3 7 5 8 9 3 11 10 6 7 4 8 5 3). There are sixteen numbers, which means that we must add 5 more random numbers. We will do that now before placing the face values into the transposition grid: (12 5 3 7 5 8 9 3 11 10 6 7 4 8 5 3 2 7 5 4 0). Before performing the transposition, we will divide this message into groups of seven: (12 5 3 7 5 8 9 | 3 11 10 6 7 4 8 | 5 3 2 7 5 4 0). We will add the numbers of the first group to those of the second group and add the new numbers of the second group to those of the third group, using modulo 13 addition. Adding the first group to the second group gives the following result: (12 5 3 7 5 8 9 | 2 3 0 0 12 12 4 | 5 3 2 7 5 4 0). Adding the second group to the third group gives the following result: (12 5 3 7 5 8 9 | 2 3 0 0 12 12 4 | 7 6 2 7 4 3 4). Now, we place these numbers into the grid to transpose them. This step is done before each transposition. We divide the numbers into groups of seven for the seven-column transpositions and groups of six for the six-column transpositions. Also, we use modulo 13 arithmetic for the face values and modulo 4 arithmetic for the suits. This increases diffusion because a change in any number will result in changes of multiple numbers after it when they are added together.

### Full Example of VICCard 5.0

For the last time, we will encrypt our favorite message Attack At Dawn. With VICCard 5.0, we will perform quite a few modifications to the plaintext before encryption. First, we will change some of the cases ATTacKaTdawn. Second, we will add some random letters to the beginning and the end jWvxxATTacKaTdawnMvHsi. Third, we will cut the message at a random point acKaTdawnMvHsijWvxxATT. Notice that we purposefully added the two x's to mark where the message begins. After all of this prep work, we can begin encryption.

**Step 1:** For Step 1, we use the substitution checkerboard method that was described in the first version. Here is the result of using the checkerboard to convert the plaintext into face values and suits:

a	c	K	a	T	d	a	W	N	M	v	H	s	i	j	W	v	x	x	A	T	T
12	8	5	12	0	9	12	1	4	8	8	4	12	8	6	1	8	6	6	1	0	0
3	3	3	3	1	0	3	1	2	0	1	0	2	2	2	1	1	0	0	0	1	1

**Step 2:** As usual, we will start with the double columnar transposition of the face values. The first columnar transposition is nothing special. It is the exact same type of transposition that we have been doing. After adding six random face values to the end so the number of face values is divisible by seven (12 8 5 12 0 9 12 1 4 8 8 4 12 8 6 1 8 6 6 1 0 0 3 4 5 3 0 3), we create diffusion based on blocks of seven (12 8 5 12 0 9 12 0 12 0 7 4 8 7 6 0 8 0 10 9 7 6 3 12 5 0 9 10). Then we perform a plain columnar transposition based on the order of A♣ through 7♣.

7♣	3♣	A♣	4♣	2♣	6♣	5♣
12	8	5	12	0	9	12
0	12	0	7	4	8	7
6	0	8	0	10	9	7
6	3	12	5	0	9	10

The result is (5 0 8 12 0 4 10 0 8 12 0 3 12 7 0 5 12 7 7 10 9 8 9 9 12 0 6 6).

The second transposition begins normally. We add two random face values so the total is divisible by six (5 0 8 12 0 4 10 0 8 12 0 3 12 7 0 5 12 7 7 10 9 8 9 9 12 0 6 6 7 7), and we create diffusion based on blocks of six letters (5 0 8 12 0 4 2 0 3 11 0 7 1 7 3 3 12 1 8 4 12 11 8 10 7 4 5 4 2 4). Before placing the face values in the grid, however, we need to create triangular sections based on the key, which is the order of A♥ through 6♥. Since we are only dealing with 30 face values, we only have to worry about the top five rows.

A♥	4♥	3♥	5♥	6♥	2♥
T	T	T	T	T	T
	T	T	T	T	T
		T	T	T	T
			T	T	T
				T	T

We first fill in the parts of the grid that are not sectioned off,

A♥	4♥	3♥	5♥	6♥	2♥
T	T	T	T	T	T
5	T	T	T	T	T
0	8	T	T	T	T
12	0	4	T	T	T
2	0	3	11	T	T

and then fill in the triangular sections:

A♥	4♥	3♥	5♥	6♥	2♥
0	7	1	7	3	3
5	12	1	8	4	12
0	8	11	8	10	7
12	0	4	4	5	4
2	0	3	11	2	4

The result is: (0 5 0 12 2 3 12 7 4 4 1 1 11 4 3 7 12 8 0 0 7 8 8 4 11 3 4 10 5 2).

Now we will do the same thing for the suits. We add five random suits so the total is divisible by seven (3 3 3 3 1 0 3 1 2 0 1 0 2 2 2 1 1 0 0 0 1 1 3 3 2 0 0 2), create diffusion based on blocks of seven (3 3 3 3 1 0 3 0 1 3 0 1 2 1 2 2 0 0 1 2 2 3 1 3 2 1 2 0), and then transpose the suits based on the order of 7♥ through K♥. The result is (3 0 2 3 3 1 2 1 3 1 2 0 1 1 1 1 0 2 2 2 3 0 0 2 3 3 0 3).

7♥	8♥	K♥	Q♥	10♥	J♥	9♥
3	3	3	3	1	0	3
0	1	3	0	1	2	1
2	2	0	0	1	2	2
3	1	3	2	1	2	0

In preparation for the second transposition, we add two random suits so the total is divisible by six (3 0 2 3 3 1 2 1 3 1 2 0 1 1 1 1 0 2 2 2 3 0 0 2 3 3 0 3 1 1), create diffusion based on blocks of six letters (3 0 2 3 3 1 1 1 1 0 1 1 2 2 2 1 1 3 0 0 1 1 1 1 3 3 1 0 2 2), and create triangular sections in the grid based on the order of 8♣ through K♣. Since there are 30 suits, we only are concerned with the first five rows of the grid.

K♣	J♣	10♣	9♣	8♣	Q♣
				T	T
					T
			T	T	T
				T	T
					T

We then fill the grid based on the triangular sections and transpose the suits.

K♣	J♣	10♣	9♣	8♣	Q♣
3	0	2	3	1	1
3	1	1	1	1	1
0	1	1	3	3	1
2	2	2	1	0	2
1	3	0	0	1	2

The result is (1 1 3 0 1 3 1 3 1 0 2 1 1 2 0 0 1 1 2 3 1 1 1 2 2 3 3 0 2 1). In summary, here are the two rows of face values and suits:

0	5	0	12	2	3	12	7	4	4	1	1	11	4	3	...
1	1	3	0	1	3	1	3	1	0	2	1	1	2	0	...
...	7	12	8	0	0	7	8	8	4	11	3	4	10	5	2
...	0	1	1	2	3	1	1	1	2	2	3	3	0	2	1

**Step 3:** For Step 3, we add the numbers from the spade lagged Fibonacci generator to the face values,

	0	5	0	12	2	3	12	7	4	4	1	1	11	4	3	...
+	13	4	2	11	5	8	10	9	7	12	6	3	1	4	6	...
=	0	9	2	10	7	11	9	3	11	3	7	4	12	8	9	...
	...	7	12	8	0	0	7	8	8	4	11	3	4	10	5	2
+	...	0	3	0	5	6	3	6	5	9	4	5	10	6	3	3
=	...	7	2	8	5	6	10	1	0	0	2	8	1	3	8	5

and we add the numbers from the diamond lagged Fibonacci generator to the suits,

	1	1	3	0	1	3	1	3	1	0	2	1	1	2	0	...
+	1	0	2	1	3	3	1	2	0	2	3	0	1	1	2	...
=	2	1	1	1	0	2	2	1	1	2	1	1	2	3	2	...

	...	0	1	1	2	3	1	1	1	2	2	3	3	0	2	1
+	...	3	0	2	0	3	2	2	1	3	1	2	3	1	3	2
=	...	3	1	3	2	2	3	3	2	1	3	1	2	1	1	3

which gives us the following face values and suits:

0	9	2	10	7	11	9	3	11	3	7	4	12	8	9	...
2	1	1	1	0	2	2	1	1	2	1	1	2	3	2	...

...	7	2	8	5	6	10	1	0	0	2	8	1	3	8	5
...	3	1	3	2	2	3	3	2	1	3	1	2	1	1	3

**Step 4:** Finally, we use the substitution checkerboard from Step 1 to convert these face values and suits into the ciphertext:

OqLPmYJwConRscJfLchjIXOTgviewvk.

## 7 Randomness Tests

The fundamental concept of cryptography is randomness. The more unpredictable a cipher is, the harder it usually is to break. For example, recall our discussion of lagged Fibonacci generators. To ensure that the lagged Fibonacci generators of VICCard are a reliable option, it was necessary to examine the randomness of the numbers that it created. We did this by focusing on the periods and the number distributions.

To test the randomness of VICCard 5.0, I encrypted six plaintexts: the Declaration of Independence, “Paul Revere’s Ride” by Henry Wadsworth Longfellow, the Gettysburg Address, the lyrics to “All I Ask Of You”, the opening to *A Tale of Two Cities*, and Psalm 23. After encrypting each plaintext using VICCard 5.0, I analyzed the letter distributions of the ciphertexts. Since we are using uppercase and lowercase letters, the ciphertexts are composed of 52 different letters. In a truly random string of letters, each of the letters will occur about  $\frac{1}{52}$  of the time. Hence, if the six ciphertexts have a letter distribution that closely resembles a random distribution, then we have strong evidence in favor of the randomness of VICCard 5.0.

### 7.1 Chi-Square Test on Ciphertexts

At this point, I enlisted the help of the Chi-Square test of fitness. This test tells us how closely a set of measured data resembles the expected data. In this case, I used the Chi-Square test to determine how closely the measured distributions of the six ciphertexts “fit” with truly random texts. Here is how the Chi-Square test works. First, we calculate the Chi-Square value of a particular ciphertext using the following formula:

$$\chi^2 = \sum_{i=1}^n \left( \frac{(O_i - E_i)^2}{E_i} \right).$$

In this formula<sup>1</sup>,  $n$  is the number of possible outcomes,  $O_i$  represents the observed number of occurrences of an outcome, and  $E_i$  represents the expected number of occurrences of an outcome. For example, consider the ciphertext of the Declaration of Independence. Since there are 52 types of letters,  $n = 52$ . The ciphertext has 6600 letters according to the breakdown in Table 12.

Letter	Number of Occurrences	Letter	Number of Occurrences
a	105	A	118
b	147	B	112
c	129	C	126
d	119	D	145
e	139	E	150
f	136	F	120
g	122	G	117
h	117	H	127
i	118	I	117
j	122	J	109
k	132	K	144
l	114	L	135
m	126	M	138
n	130	N	133
o	126	O	148
p	134	P	154
q	126	Q	115
r	113	R	124
s	122	S	138
t	114	T	127
u	125	U	117
v	143	V	122
w	117	W	119
x	139	X	130
y	135	Y	112
z	117	Z	136

Table 12: Letter Distribution of the Declaration of Independence

To calculate this ciphertext's Chi-Square value, we first calculate each of the individual Chi-Square terms. For example, consider the letter a. This letter occurs 105 times. This is the observed number of occurrences,  $O_i$ . In a truly random string of letters, the letter a would occur about  $\frac{1}{52}$  of the time. Since there are 6600 letters in the ciphertext of the Declaration of Independence, the expected number of occurrences  $E_i$  is  $\frac{6600}{52} \approx 126.923$ . Using the formula above, the Chi-Square term for a is

$$\frac{(O_i - E_i)^2}{E_i} \approx \frac{(105 - 126.923)^2}{126.923} \approx 3.7867.$$

This calculation is performed for each of the 52 letters, and the final Chi-Square value is the sum of all these 52 calculations:  $\chi^2 \approx 54.4558$ .

<sup>1</sup> $\chi^2$  is the symbol for the Chi-Square value.

What does  $\chi^2$  tell us? This number signifies how well the data emulates perfect randomness by measuring the level of deviation from perfect randomness. The larger the Chi-Square value, the more the data deviates. To determine the amount of deviation, we use the Chi-Square value to calculate the associated  $p$ -value. Looking up the above  $\chi^2$  in a  $p$ -value table, we see that this data has a  $p$ -value of 0.3444. This  $p$ -value means the following: if I create a string of 6600 letters by choosing each letter at random, there is a 0.3444 probability of getting a string of letters that has a Chi-Square value of 54.4558. In other words, there is a 0.3444 probability that the Declaration of Independence ciphertext is random. The relevance of the  $p$ -value is in its ability to measure the level of randomness in a ciphertext.

In order to have a respectable sample size, I encrypted six plaintexts with six different keyed decks and performed a Chi-Square test on each ciphertext. Table 13 contains a summary of the test data.

Plaintext (length)	Ciphertext Length	$\chi^2$	$p$ -value
Psalm 23 (461)	468	42.2222	0.8044
Opening to <i>A Tale of Two Cities</i> (475)	480	52.1333	0.4296
"All I Ask Of You" (813)	822	57.6983	0.2415
Gettysburg Address (1149)	1158	56.7703	0.2688
"Paul Revere's Ride" (4054)	4062	39.8552	0.8705
Declaration of Independence (6591)	6600	54.4558	0.3444

Table 13: First Round of Chi-Square Test Results

After compiling this data, I encrypted these six plaintexts a second time, using a different keyed deck for each encryption. Table 14 contains the data from this second round of tests.

Plaintext (length)	Ciphertext Length	$\chi^2$	$p$ -value
Psalm 23 (461)	468	53.1111	0.3929
Opening to <i>A Tale of Two Cities</i> (475)	480	41.3000	0.8320
"All I Ask Of You" (813)	822	37.3285	0.9237
Gettysburg Address (1149)	1158	63.5060	0.1123
"Paul Revere's Ride" (4054)	4062	45.6928	0.6838
Declaration of Independence (6591)	6600	47.2703	0.6226

Table 14: Second Round of Chi-Square Test Results

## 7.2 Chi-Square Test on One-Time Pads

A second randomness test is a slight variation of the previous Chi-Square test. The first Chi-Square test measures the randomness of the ciphertexts. The second Chi-Square test measures the randomness of the associated one-time pads.

A one-time pad is a random string of numbers that is used to encrypt a message. For example, suppose that I want to encrypt `attack at dawn`. Since my plaintext is 12 letters long, I randomly choose a string of 12 numbers to be my one-time pad: 5 3 6 14 22 19 10 8 2 23 11 15. To encrypt the plaintext, I "add" the one-time pad to the plaintext. Since I cannot add numbers to letters, I first convert `attack at dawn` to numbers as per the following: a is represented with the

number 1, b becomes 2, c becomes 3, and so forth. Now, I can add the one-time pad to the plaintext.

	a	t	t	a	c	k	a	t	d	a	w	n
	1	20	20	1	3	11	1	20	4	1	23	14
+	5	3	6	14	22	19	10	8	2	23	11	15
=	6	23	26	15	25	4	11	2	6	24	8	3
	f	w	z	o	y	d	k	b	f	x	h	c

Converting the sum back into letters gives us the ciphertext *fwzoyd kb fxhc*. The reason that we are concerned with one-time pads is because it is the only proven way to create perfect encryption. This is because the key is a truly random string of numbers, and there is no way to crack the cipher other than by trying every key by brute-force.

In this example, we applied a one-time pad to a plaintext in order to generate a ciphertext. Consider doing the reverse process. If we take a ciphertext that we have generated and subtract the plaintext from it, we get the one-time pad that was used to encrypt the plaintext. However, let's say that the plaintext was not encrypted with a one-time pad. In this case, subtracting the plaintext from the ciphertext tells us that the encryption process has the same effect as the calculated one-time pad. If this one-time pad is sufficiently random, this would act as evidence in favor of the cipher's security.

For my second test, I encrypted the same six ciphertexts using six different keys. Instead of performing another Chi-Square test on the ciphertexts, I first subtracted the plaintexts from the ciphertexts in order to find the six one-time pads. I then carried out a Chi-Square test on each one-time pad. Table 15 lists the results. Since the plaintexts are slightly shorter than the ciphertexts, the one-time pads are the same length as the corresponding plaintexts.

Plaintext	$\chi^2$	<i>p</i> -value
Psalm 23	49.1866	0.5460
Opening to <i>A Tale of Two Cities</i>	60.4358	0.1717
"All I Ask Of You"	50.5326	0.4921
Gettysburg	29.0783	0.9942
"Paul Revere's Ride"	32.1944	0.9817
Declaration of Independence	63.8245	0.1072

Table 15: First Round of Chi-Square Test Results (One-Time Pad)

Table 16 contains the results from a second round of tests in which the same six plaintexts were encrypted with six different decks.

Plaintext	$\chi^2$	<i>p</i> -value
Psalm 23	62.0456	0.1382
Opening to <i>A Tale of Two Cities</i>	63.7200	0.1089
"All I Ask Of You"	47.2066	0.6251
Gettysburg	52.0688	0.4321
"Paul Revere's Ride"	40.7884	0.8463
Declaration of Independence	60.8264	0.1631

Table 16: Second Round of Chi-Square Test Results (One-Time Pad)

### 7.3 The Washington Test

In the previous tests, I encrypted different plaintexts with different deck keys. With this third test, I encrypted different plaintexts with the same keyed deck. I took the first 29,120 letters of George Washington's Farewell Address and divided them into 28 groups of 1040 letters. I then encrypted each group using the same deck to create 28 ciphertexts of length 1044. Table 17 contains the Chi-Square values and  $p$ -values of each ciphertext. The average  $p$ -value is 0.4614.

	$\chi^2$	$p$ -value
1	49.49425287	0.533610953
2	43.31800766	0.769024139
3	55.8697318	0.29694992
4	65.63218391	0.08162056
5	60.651341	0.166941401
6	51.5862069	0.450724746
7	64.13793103	0.10236771
8	59.75478927	0.187574286
9	58.65900383	0.215146577
10	45.01149425	0.709235389
11	36.5440613	0.936595831
12	48.79693487	0.561608159
13	49.59386973	0.529616108
14	52.38314176	0.420092715
15	35.8467433	0.946712769
16	53.57854406	0.375647609
17	42.81992337	0.785476088
18	64.9348659	0.090831388
19	63.54022989	0.111762895
20	68.72030651	0.049573757
21	52.38314176	0.420092715
22	55.47126437	0.309943572
23	45.90804598	0.675579632
24	45.21072797	0.701860096
25	62.84291188	0.123565899
26	47.20306513	0.625220692
27	40.92720307	0.842450584
28	38.53639847	0.900501941

Table 17: Chi-Square Test Results of Washington's Farewell Address

### 7.4 Interpreting the Results

The rationale for performing these tests is as follows. An English plaintext tends to have a predictable distribution. Letters such as e and t occur very frequently, whereas letters such as q and z are comparatively rare. These tests examine whether VICCard can transform a typical English letter distribution into something more like pure randomness.

Executing these Chi-Square tests provides reasonable evidence as to VICCard 5.0's ability to turn an English plaintext into a random message. Notice that most of the ciphertexts and one-time pads have respectable  $p$ -values with the occasional outlier. The first and second Chi-Square tests on the ciphertext yielded average Chi-Square values of 0.4932 and 0.5945, respectively. In other words, on average

there is about a 50/50 chance that the ciphertext is random. This is further reflected by the average  $p$ -value of 0.4614 in the data from Washington's Farewell Address. The first and second Chi-Square tests on the one-time pads yielded average Chi-Square values of 0.5488 and 0.3856, respectively.

Fortunately, many of the  $p$ -values are very high. Unfortunately, there are just as many  $p$ -values that are less than optimal. Still, this is not necessarily a bad thing. These low  $p$ -values are cause for concern if they are the result of a bias within VICCard 5.0. In other words, is there a security weakness of VICCard 5.0 that is making it give us low  $p$ -values?

To ensure that this is not the case, I performed what is called a drill-down test. I randomly picked the ninth group from Washington's Farewell Address, encrypted it differently, and found that the letter D occurred 31 times, a recognizable deviation from the expected  $\frac{1044}{52} \approx 20.0769$  times. I then tracked each D through the encryption process to see if there was a feature of the cipher that caused a bias towards encrypting D more than any other letter. Given the extensive amount of substitutions that are performed (the checkerboard, the cipher block chaining, and the lagged Fibonacci generators), I was unable to find any factors that steered the cipher towards the letter D.

Instead, it appears that the high Chi-Square values are the result of an expected level of variation. For example, the second Gettysburg Address ciphertext has a Chi-Square value of 63.5060 and a  $p$ -value of 0.1123. Since the ciphertext had 1158 letters, each letter was expected to occur about  $\frac{1158}{52} \approx 22.2692$  of the time. The high Chi-Square is not because every letter significantly deviates from occurring 22.2692 of the time. Instead, there were 7 outlying letters that occurred about 10 times more or less than the expected number. This is an allowable level of variation and is not necessarily a sign of a weakness.

To further confirm this, we will use the Empirical Rule. The Empirical Rule states that with normal data distributions and binomial data distributions, the data tends to follow a bell-shaped curve. Numerically, this means that about 68% of the data falls within one standard deviation of the mean, about 95% of the data falls within two standard deviations, and nearly all of the data falls within three standard deviations<sup>2</sup>. For example, consider the encryption of the Declaration of Independence. Since we expect each letter to occur  $\frac{1}{52}$  of the time and since there are 6600 letters in the ciphertext, the standard deviation is

$$\sqrt{\left(\frac{1}{52}\right)\left(1 - \frac{1}{52}\right)\left(\frac{1}{6600}\right)} \approx 0.0016905.$$

Furthermore, the expected number of occurrences of each letter is  $\frac{6600}{52} \approx 126.92$ . This means that we expect 68% of the data to be within

$$(0.0016905)(6600) \approx 11.16$$

---

<sup>2</sup>The symbol for standard deviation is  $\sigma$ .

of 126.92, 95% of the data to be within

$$(2)(0.0016905)(6600) \approx 22.31$$

of 126.92, and almost all of the data to be within

$$(3)(0.0016905)(6600) \approx 33.47$$

of 126.92. Tables 18 through 21 confirm that the data for the six plaintexts follow this trend.

Plaintext	Percent in $\sigma$	Percent in $2\sigma$	Percent in $3\sigma$
Psalm 23	69.23%	96.15%	100.00%
Opening to <i>A Tale of Two Cities</i>	69.23%	96.15%	100.00%
“All I Ask Of You”	63.46%	94.23%	100.00%
Gettysburg	61.54%	96.15%	100.00%
“Paul Revere’s Ride”	71.15%	100.00%	100.00%
Declaration of Independence	67.31%	96.15%	100.00%

Table 18: Empirical Rule for First Round of Chi-Square Test Results

Plaintext	Percent in $\sigma$	Percent in $2\sigma$	Percent in $3\sigma$
Psalm 23	55.77%	96.15%	98.08%
Opening to <i>A Tale of Two Cities</i>	69.23%	98.08%	100.00%
“All I Ask Of You”	76.92%	100.00%	100.00%
Gettysburg	61.54%	86.54%	100.00%
“Paul Revere’s Ride”	69.23%	94.23%	100.00%
Declaration of Independence	73.08%	96.15%	98.08%

Table 19: Empirical Rule for Second Round of Chi-Square Test Results

Plaintext	Percent in $\sigma$	Percent in $2\sigma$	Percent in $3\sigma$
Psalm 23	69.23%	92.31%	100.00%
Opening to <i>A Tale of Two Cities</i>	65.38%	94.23%	98.08%
“All I Ask Of You”	69.23%	98.08%	100.00%
Gettysburg	75.00%	100.00%	100.00%
“Paul Revere’s Ride”	80.77%	98.08%	100.00%
Declaration of Independence	69.23%	90.38%	98.08%

Table 20: Empirical Rule for First Round of Chi-Square Test Results (One-Time Pad)

Plaintext	Percent in $\sigma$	Percent in $2\sigma$	Percent in $3\sigma$
Psalm 23	71.15%	96.15%	98.08%
Opening to <i>A Tale of Two Cities</i>	61.54%	92.31%	98.08%
“All I Ask Of You”	73.08%	94.23%	100.00%
Gettysburg	63.46%	98.08%	100.00%
“Paul Revere’s Ride”	75.00%	96.15%	100.00%
Declaration of Independence	63.46%	92.31%	100.00%

Table 21: Empirical Rule for Second Round of Chi-Square Test Results (One-Time Pad)

## 8 Closing Thoughts

Ernő Rubik, the inventor of the Rubik's cube, had a fond way of describing his creation. He affirmed that the Rubik's cube "embodies the tension of our most basic contradictions: simplicity and complexity... and so forth" [14]. The cube is simple because a brief glance is enough to figure out the goal of the puzzle. Only a few seconds are needed to discover how the puzzle moves. However, determining the correct sequence of these moves is what makes it complex. It is this blend of simplicity and complexity that has driven the Rubik's cube's worldwide popularity [14].

This is the driving force behind playing card ciphers. A deck of cards is compact, portable, and readily accessible. However, its disarming simplicity is belied by the 225-bits of entropy that are packed into it. Furthermore, drawing out this wellspring of entropy is far from straightforward. The nascent field of playing card ciphers has brought to light many fascinating methods of doing so. In this research, I have presented my own contribution to this developing field.

VICCard 5.0 combines numerous cryptographic techniques. Certain features are reminiscent of VIC, which intensely added the FBI during the Cold War. VIC-Card 5.0 also makes unique contributions of its own. It creates a novel substitution checkerboard, and it affords the incredible convenience of containing numerous keys in a single deck. In these regards, VICCard 5.0 distinguishes itself among other playing card ciphers. Furthermore, as demonstrated by the Chi-Square tests, it has the potential to create ciphertexts with respectable levels of randomness.

In a time when computer ciphers have become the industry standard, it is useful to not completely discount low-tech options. Analyzing the features that made hand ciphers secure for hundreds of years continues to inform and inspire our understanding of information security as a whole. In creating VICCard 5.0, my goal has been to show that computer ciphers have not entirely superseded hand ciphers. Additional innovation is still yielding formidable ciphers and fascinating cryptographic principles.

## References

[1] Jim Dwyer. Sidelight to a Spy Saga: How a Brooklyn Newsboy's Nickel Would Turn Into a Fortune. <https://www.nytimes.com/2015/11/04/nyregion/how-a-brooklyn-newsboys-nickel-helped-convict-a-soviet-spy.html>, November 2015. Accessed July 8, 2020.

[2] FBI. Hollow Nickel/Rudolf Abel. <https://www.fbi.gov/history/faithful-cases/hollow-nickel-rudolph-abel>. Accessed July 8, 2020.

[3] FermiLab. Physics Questions People Ask Fermilab. <https://www.fnal.gov/pub/science/inquiring/questions/atoms.html>, April 2014. Accessed July 20, 2020.

- [4] Stephen Fry. Qi Card Shuffling - 52 Factorial. <https://www.youtube.com/watch?v=SLIvwtIuC3Y>, November 2012. Accessed July 23, 2020.
- [5] Edy Victor Haryanto, Muhammad Zulfadly, Daifiria, Muhammad Barkah Akbar, and Ivy Lazuly. Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification. *Journal of Physics: Conference Series*, 1361, 2019.
- [6] Jeffrey A. Hill. Chaocipher: Analysis and Models. <http://www.chaocipher.com/HillDocs/H03H09.pdf>, April 2009. Accessed June 8, 2020.
- [7] David Kahn. Number One From Moscow. <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol15no4/html/v05i4a09p\0001.htm#top>, July 2008. Accessed July 8, 2020.
- [8] James Lyons. Cryptanalysis of the columnar transposition cipher. <http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-columnar-transposition-cipher/>, 2012. Accessed July 23, 2020.
- [9] Matthew McKague. Design and analysis of RC4-like stream ciphers. Master's thesis, University of Waterloo, Waterloo, ON, Canada, 2005.
- [10] Sanjay Kumar Pal, Bimal Datta, and Amiya Karmakar. Cryptography and Network Security: A Historical Transformation. *SCHOLEDGE International Journal Of Multi-disciplinary & Allied Studies*, 7(2):30-44, 2020.
- [11] Isaac Reiter and Eric Landquist. Determining Biases in the Card-Chameleon Cryptosystem. *Communications on Number Theory and Combinatorial Theory*. Vol. 2, Article 1. Available at: <https://research.library.kutztown.edu/contact/vol2/iss1/1>.
- [12] Moshe Rubin. The Chaocipher challenge: Further work in progress. <http://www.mountainvistasoft.com/chaocipher/chaocipher-001.htm>, November 2009. Accessed July 23, 2019.
- [13] Moshe Rubin. John F. Byrne's Chaocipher Revealed: An Historical and Technical Appraisal. *Cryptologia*, 35:328-379, 2011.
- [14] Ian Scheffler. *Cracking the Cube*. Touchstone, New York, New York, 2016.

[15] Aaron Toponce. The Chaocipher Cipher. <https://aarontoponce.org/wiki/crypto/card-ciphers/chaocipher>, October 2018. Accessed May 24, 2019.

[16] Aaron Toponce. Playing card ciphers. <https://aarontoponce.org/wiki/crypto/card-ciphers>, October 2018. Accessed May 28, 2020.

[17] Wikipedia contributors. VIC cipher — Wikipedia, the free encyclopedia, July 2020. Accessed June 3, 2020.

[18] Wikipedia contributors. Transposition cipher — Wikipedia, the free encyclopedia, October 2020. Accessed June 3, 2020.

### **Acknowledgements**

I gratefully acknowledge the support of the Honors Program of Kutztown University of Pennsylvania, for which this paper is intended. Also, I am very grateful for the opportunities provided by the KUBEARS grant (Kutztown University Bringing Experience About Research to Students). Much of the preliminary work for this research was completed under this grant in the summer of 2019. Most importantly, I would like to thank my research advisor, Dr. Eric Landquist. I am remarkably fortunate to have had Dr. Landquist as my professor and mentor throughout my undergraduate experience.

### **Editor's Note**

Isaac Reiter's work won second place and the People's Choice Award at the (virtual) 43<sup>rd</sup> Biennial Convention hosted by the University of Central Missouri in Warrensburg, Missouri, April 15-17, 2021.

# ***That's Impossible! An Exploration of Three Famous Impossibilities***

Lisa Reed, *student*

TN Gamma

Union University  
Jackson, TN 38305

## **Abstract**

The three famous ancient Greek construction problems involve using only a straight-edge and compass to double the cube, trisect an angle, and square the circle. Attempting these constructions have captivated geometers for centuries. It was not until the nineteenth century that Wantzel proved the impossibility of doubling the cube and trisecting an angle and Lindemann completed the proof of the impossibility of squaring the circle. While the problems seem geometric in nature, proving the impossibility of these constructions requires abstract algebra. This paper discusses the idea of constructible numbers, i.e., lengths that can be constructed using only a compass and straightedge and will introduce two important theorems concerning constructible numbers. In addition, a proof of the transcendence of  $\pi$  will be presented. Finally, based on these theorems and lemmas, proofs of the three impossibilities will be presented.

## **Contents**

1 Introduction	38
1.1 Statement of the Impossibilities	38
1.2 Rules	38
1.2.1 Collapsible vs. Noncollapsible Compasses	40
2 History of the Problems	41
2.1 Background	41
2.2 Historical Origins	43
2.3 Attempts and “Solutions”	44
3 Algebra Background	47
3.1 Rings and Fields	47
3.2 Polynomials	47
3.3 Extension Fields	48
3.4 Algebraic Numbers	48
4 Constructible Numbers	48
4.1 Two Important Theorems	50
5 Transcendence of $\pi$	52
6 Impossibility Proofs	64

6.1 Doubling the Cube	64
6.2 Trisecting an Arbitrary Angle	64
6.3 Squaring the Circle	65
References	65

## 1 Introduction

Construction problems using a compass and straightedge became popular during the time of the Ancient Greeks. From existing points and using only a compass and straightedge, a person can connect any two points to create a line, or place the compass on any point to create a circle centered at that point with a radius of an existing line segment. However, when following the classical construction rules, some geometric constructions become impossible to achieve with only straightedge and compass. This paper will discuss three famous impossibilities – that of doubling the cube, trisecting an arbitrary angle, and squaring the circle. The book *Abstract Algebra and Famous Impossibilities* provides a basis for this work [1].

### 1.1 Statement of the Impossibilities

The first problem is to construct a cube with twice the volume of a given cube. For example, there exists a cube with sides of length 1; so its volume is  $1^3 = 1$  cubic unit. Thus a cube of twice that volume would be 2 cubic units with sides of length  $\sqrt[3]{2}$ . This is illustrated by figure 1.

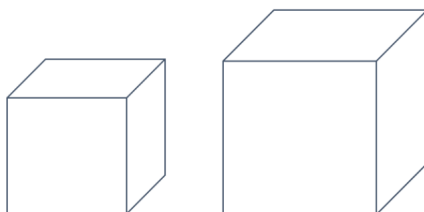


Figure 1: Doubling the cube

The second problem is to trisect an arbitrary angle. While it may be easy to do this for angles of certain measures, this problem is asking for a way to trisect any arbitrary angle regardless of its measure. Figure 2 illustrates this problem.

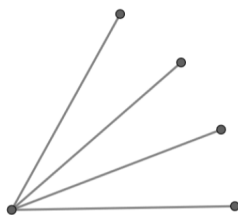


Figure 2: Trisecting an angle

The third problem is to construct a square with the same area as a circle with a given radius. Again, for example assume there exists a circle of radius 1; so its area would be  $\pi \times 1^2 = \pi$ . Thus, a square with the same area would have sides of length  $\sqrt{\pi}$ . This is shown in figure 3.

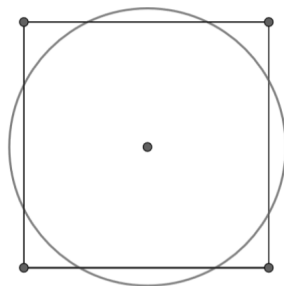


Figure 3: Squaring the circle

## 1.2 Rules

For construction problems, one needs basic rules concerning the tools and methods that can be employed to create points and lines; else one could simply measure or guess a distance, create a point, and draw whatever is needed to complete the construction. Classical construction problems always begin with some existing points, and possibly line segments or circles. In Euclid's *Elements*, the postulates limit the construction of geometric objects to using only the compass and unmarked straightedge to form lines and circles [4]. The classical rules regarding the construction of these three problems follow from *Elements*.

There are two ways one can form new points from existing points: circles, and lines or line segments. The first way is how people often think of how to make a line – take two existing points ( $P_i$  and  $P_j$  in Figure 4) and connect them with a line. Where this line intersects existing objects (the dotted circle and line), new points are created ( $X$ ,  $Y$ , and  $Z$ ).

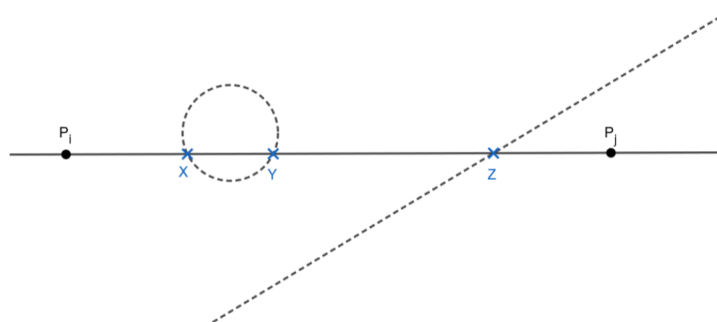


Figure 4: New points from a line

The other way in which to get new points is by drawing a circle, as shown in Figure 5. Say there exists points  $P_j$ ,  $P_k$ , and  $P_i$ , and the dotted line and circle shown. Then one can set the compass at point  $P_i$  and draw a circle of radius the

length of line segment  $P_j P_k$ . Where this circle intersects existing lines and circles, new points are created ( $W, X, Y, Z$ ).

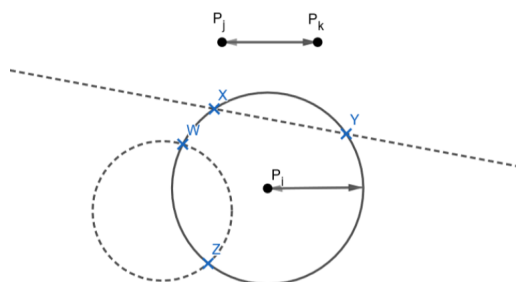


Figure 5: New points from a circle

These two ways are the only allowable methods to create new points, and lines and circles can only be constructed by using points.

With these rules in place, we can define what a constructible number is.

**Definition 1.** A real number  $\gamma$  is constructible if, starting with two points  $P_1, P_2$  one unit length apart and doing a finite number of the above two methods of creating new points, we can create new points  $P_i, P_j$  such that the length of  $\overline{P_i P_j}$  is  $|\gamma|$  units.

### 1.2.1 Collapsible vs. Noncollapsible Compasses

For the classical problems, the compass is viewed as the Ancient Greeks viewed it: as collapsing when lifted from the page. This means it cannot be used to copy a distance  $AB$  by placing it centered at  $A$  with radius  $AB$ , then lifting the compass to place at another point, say  $C$ , and marking off the distance  $AB$ . Instead, one can imagine a string being used as a compass, which when lifted from the page collapses and loses the radius first marked. In the modern day, compasses are usually noncollapsible, meaning they can keep their measurement when lifted from the page. At first thought, it may seem that the collapsible compass is more limited than the noncollapsible compass; this is not true. In fact, any construction a noncollapsible compass can do the collapsible compass can also do, just requiring more steps. Thus, we will use a noncollapsible compass for the constructions in this paper, with the knowledge that they can be performed via a collapsing compass if need be [6]. The following theorem will demonstrate this fact, referencing figure 6.

**Theorem 2** (Collapsible Compass Theorem). Given a point  $A$  and a line segment  $\overline{BC}$ , to construct a point  $D$  such that line segment  $\overline{AD}$  can be constructed and  $\overline{AD} \cong \overline{BC}$ .

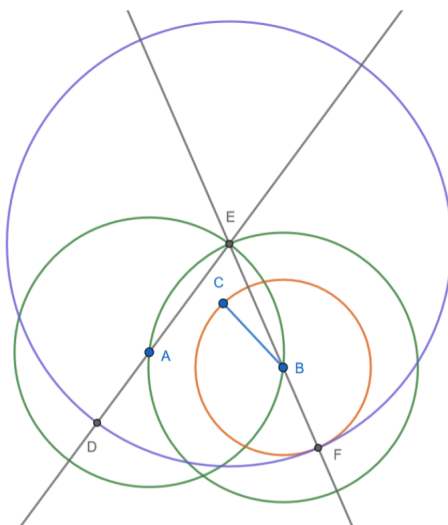


Figure 6: Figure to illustrate Theorem 2

*Proof.* Construct an equilateral triangle  $\triangle ABE$  with base  $\overline{AB}$ . This is a construction shown in Euclid's *Elements* and thus can be performed. Construct a circle centered at  $B$  through  $C$ . Let  $F$  be the point at which this circle intersects  $\overrightarrow{EB}$  such that  $B$  is between  $E$  and  $F$ . Construct a circle centered at  $E$  through  $F$ . Let  $D$  be the point at which this circle intersects  $\overrightarrow{EA}$ .

As  $\overline{ED}$  and  $\overline{EF}$  are both radii of the same circle,  $\overline{ED} \cong \overline{EF}$ , so  $ED = EF$ . Furthermore, as  $\triangle ABE$  is an equilateral triangle,  $\overline{EA} \cong \overline{EB}$  and  $EA = EB$ . Now, as  $A$  is between  $E$  and  $D$ , and  $B$  is between  $E$  and  $F$ , we have that  $EA + AD = ED$  and  $EB + BF = EF$ . As  $EF = ED$ , we get  $EA + AD = EB + BF$ . Since  $EA = EB$ , we can subtract those and have  $AD = BF$ . Finally, note that as  $BF$  and  $BC$  are both radii of the same circle,  $\overline{BF} \cong \overline{BC}$  and  $BF = BC$ . Thus,  $AD = BC$ , and we have the line segment requested. ■

## 2 History of the Problems

### 2.1 Background

The three famous problems discussed in this paper – doubling the cube, trisecting an arbitrary angle, and squaring the circle – all originated or became popular in the 5th century B.C. in ancient Greece [5]. Part of the appeal of these problems is their apparent simplicity. It is straightforward to understand what each construction seeks to accomplish, and there are only the two basic rules of Euclidean construction to follow. In ancient Greece, there was even a word used to describe those who dedicated their time to attempting to solve the problem of squaring the circle. This word was  $\tau\epsilon\tau\rho\alpha\omega\nu\iota\zeta\epsilon\iota\nu$  “Tetragonidzein”, which translates as “to occupy oneself with the quadrature” [1].

However simple these problems may seem, they proved to be extremely difficult, if not impossible, to accomplish using only straightedge and compass while

following the construction rules. In fact, mathematicians soon started to suspect they were impossible, and began attempting the problems with marked straight-edge, other tools, and/or breaking the rules. Many important discoveries in the field of geometry were made in attempts to solve these problems. These discoveries include the conic sections, as well as many cubic, quartic, and transcendental curves [4]. The later section on “Attempts and Solutions” will describe some of these alternate solutions.

It is harder to prove something is impossible than to prove it is possible. As an example, considering the problem of “construct a circle.” To prove it possible, one must only describe one way to construct a circle. But to prove it impossible, it is not enough to have even 500 ways that do not work and be unable to find a method to construct a circle. There is always the possibility, however slight, that the next method tried will work. Thus, it takes more effort to prove impossibility. In ancient Greece, when the three construction problems first became popular, there were no ways found to perform the constructions abiding by the Euclidean rules. There is reason to believe they thought it was impossible as they began trying other methods and utilizing more tools than the unmarked straightedge and compass alone. However, they were not able to prove that the constructions were impossible.

This state of not being able to find a solution to the three construction problems, yet not being able to prove the impossibility of such solutions, remained the case for almost 2,000 years. The problems also continued to intrigue mathematicians, both professional and amateur, as they attempted to settle the question of impossibility. Around 320 A.D., Pappus of Alexandria wrote *The Collection*. In Book III, he discussed the three famous construction problems, and gave solutions by using other means than simply straightedge and compass. In his work, Pappus categorized problems as being “plane,” “solid,” or “linear.” Plane problems are solvable with circles and lines only; solid problems require conic sections; and linear problems need curves other than circles, lines, and conics to solve them. Of interest, Pappus classified doubling the cube and trisecting an angle as solid problems, and squaring the circle as a linear problem. Thus, he implies that there is no solution to the problems following the classical rules of only using compass and straightedge [2]. Centuries later, in 1775, the Paris Academy passed a resolution – *Histoire de l’Académie royale, année 1775* p.61—to prohibit the examination of proposed solutions to the three problems, as this was taking too much time that could have been used more productively on other problems [1].

While doubling the cube, trisecting an arbitrary angle, and squaring the circle are problems which are geometric in nature, the surprising fact is that proving the constructions to be impossible requires the use of abstract algebra. As abstract algebra was not discovered until the 19th century, this meant the impossibility proofs were not able to be done until then. In 1837, Pierre Wantzel published his paper “Recherches sur les moyens de reconnaître si un problème de Géométrie peut se résoudre avec la règle et le compas” in the *Journal de Mathématiques Pures et Appliquées*, proving the impossibility of doubling the cube and trisecting

an arbitrary angle [8]. The proof of the impossibility of squaring the circle was more complicated, as it necessitated proving the transcendence of the real number  $\pi$ . This was accomplished by Ferdinand von Lindemann in 1882 in his paper “Über die Zahl  $\pi$ ”, published in *Mathematische Annalen* [7].

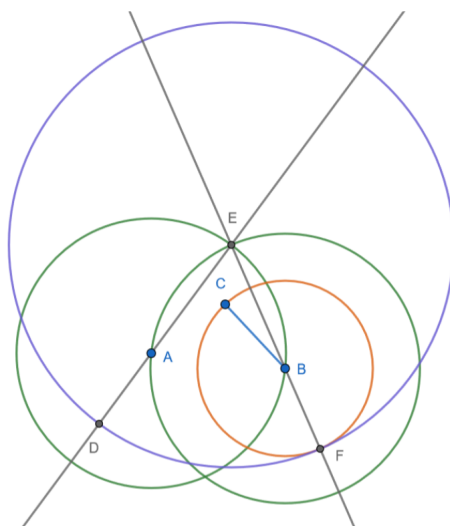


Figure 6: Figure to illustrate Theorem 2

## 2.2 Historical Origins

There are several stories behind the origin of the first construction problem—that of doubling the cube. One such explanation concerns the tomb of King Minos’s son Glaucus. He had died, and King Minos had constructed a tomb for him in the shape of a cube. An unknown Greek poet was unsatisfied with the size of the tomb and wrote that it should be doubled—a feat which he claimed could be accomplished by simply doubling each side of the tomb’s dimensions. However, when the sides of a cube are doubled, the surface area of that cube is now four times as large, and the cube’s volume is eight times the original volume, not doubled. This realization led to many geometers becoming interested in finding a way in which one could double a cube with compass and straightedge [4] [1].

Another explanation for the origins of the problem of doubling the cube comes from the time of Pericles in ancient Greece. There was a great plague at that time, killing almost a fourth of the population of Athens. Supposedly, a group of people went to the oracle of Apollo at Delos, seeking wisdom on how to stop this dreadful plague. The oracle told them that they must double the cubical altar to Apollo, and then the plague would end. The messengers quickly went to the altar and doubled each of its dimension. However, doubling each side of a cube results in a cube with eight times the volume, and not double. Thus, the plague was not averted. From this, the problem of doubling a cube by using straightedge and compass was created called the “Delian problem,” a reference to the oracle of Apollo at Delos [4]. The origins of the other two problems, trisecting an arbitrary

angle and squaring the circle, do not have as interesting of stories. It is likely that the problem of trisecting an arbitrary angle arose from attempts to construct a regular 9-sided polygon. This construction would require trisecting a  $60^\circ$  angle [1] [4]. The third problem of squaring the circle is sometimes called the quadrature problem, which refers to its probable origin in attempting to calculate the area enclosed by a circle. The problem itself has been around since before the ancient Greeks; in 1800 B.C. Egyptians attempted to square a circle by making the sides of the square  $\frac{8}{9}$  the length of the circle's diameter. The first mention of this problem in Greek mathematics is by Anaxagoras, who apparently used the problem as a means to occupy himself while in prison [2] [4].

### 2.3 Attempts and “Solutions”

While actually completing the construction problems of doubling the cube, trisecting an arbitrary angle, and squaring the circle eventually proved to be impossible, due to the popularity of the problems, there were many attempts made to solve them. When doing the constructions following the Euclidean construction rules proved difficult, many geometers attempted to discover new ways to accomplish the task.

The first construction problem of doubling the cube, or the Delian problem, has a lengthy history of attempts to solve it. While actually completing the construction with only straightedge and compass is impossible, as will be shown later on, attempts to do so resulted in many mathematical discoveries. The first major progress towards this problem came around 430 B.C. by Hippocrates. He reduced the problem to the construction of two mean proportionals. A *mean proportional* of two positive numbers  $a$  and  $b$  is the positive value of  $x$  such that  $\frac{a}{x} = \frac{x}{b}$ . Thus,  $a$  is to  $x$  as  $x$  is to  $b$ , and we can write  $x^2 = ab$ . Using modern algebraic notation, we let  $s$  be the length of a side of the original cube, and  $x$  the length of a side of the doubled cube. Then finding two mean proportionals results in the equations  $y^2 = 2sx$  and  $x^2 = sy$ . Solving for  $y$  yields  $x^3 = 2s^3$ . This  $x$  will be the length of a side of the doubled cube with the original cube having sides of length  $s$  [4]. This reduction of the problem, while not immediately helpful, is actually used in the eventual proof of the impossibility of doubling the cube. In ca. 400 B.C., Archytas developed a solution involving higher geometry. His three-dimensional proof involved the intersection of a right circular cylinder, torus, and right circular cone [4]. Later, Eudoxus also solved the problem, again by going beyond straightedge and compass, but unfortunately his solution has been lost [4]. In ca. 350 B.C., Menaechmus discovered conic sections as he sought a curve that had the necessary properties for use in doubling the cube [2]. Eratosthenes and Nicomedes, ca. 203 B.C., both used mechanical contrivances to double the cube. Also around that time, Apollonius gave a new proof of a method to double the cube using more than compass and straightedge. In ca. 180 B.C., Diocles discovered the cissoid curve (figure 7), which he used to accomplish the doubling [4].



Figure 7: Cissoid Curve

Regarding the second problem of trisecting an arbitrary angle, the ancient Greeks were able to show that by using a compass and a marked instead of unmarked straightedge, any angle could be trisected. In addition to using a marked straightedge, many curves were also discovered and found useful in trisecting angles. In ca. 240 B.C., Nicomedes used the conchoid curve (figure 8) for trisecting angles.

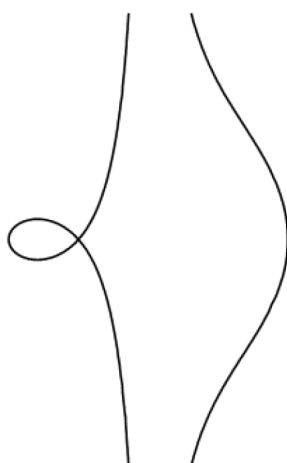


Figure 8: Conchoid Curve

In roughly 425 B.C. Hippias of Elis discovered the trisectrix curve, (figure 9), which he used to trisect an arbitrary angle [4]. This same curve was also used later to square the circle. The 3rd century B.C. renowned Greek mathematician Archimedes was, like many others, interested in solving the three problems. He succeeded in trisecting an arbitrary angle and squaring the circle, of course breaking the rules like all others.

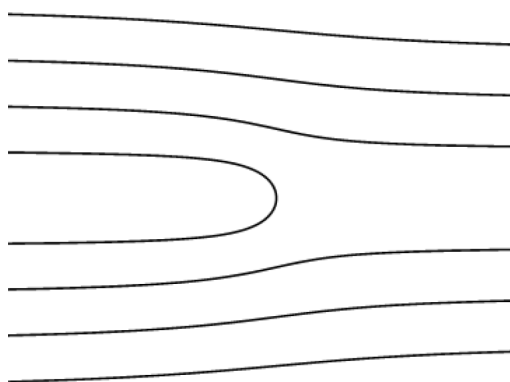


Figure 9: Trisectrix Curve

The extra object he used was what is now called the Archimedean spiral, (figure 10). This spiral is the locus of a point that is moving uniformly away from the endpoint of a ray or half line while that ray or half line is also rotating uniformly about its endpoint. In modern day polar coordinates the equation of an Archimedean spiral is given by  $r = a\theta$  [2]. By using the spiral, Archimedes was able to complete the trisection of an arbitrary angle.

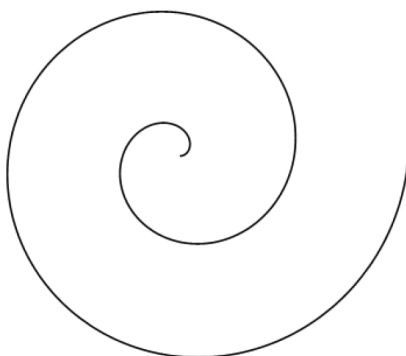


Figure 10: Spiral of Archimedes

Conics can also be used to trisect angles, however the proof of trisection involving conics was not completed until around 300 A.D. by Pappus [4]. In addition to curves, many mechanical inventions have been created for the purpose of angle trisection, including the tomahawk which was first published in 1835 [4].

As mentioned previously, the first Greek person recorded to have worked on the problem of squaring the circle was Anaxagoras in around 450 B.C.. However, his contributions to this problem are unknown [4]. Around the same time, Hippocrates of Chios successfully squared some special types of lunes. He hoped that squaring a lune would become a first step towards squaring the circle, but it did not [2] [4]. Dinostratus, brother to Menaechmus who had worked on doubling the cube, “solved” the problem of squaring the circle. Like his brother, Dinostratus knowingly broke the rules of allowing only lines and circles to be used in the construction. His proof used the trisectrix that Hippias had discovered in his attempts

to trisect an angle. With this trisectrix, he was able to show how one could square the circle. This curve later became known as the quadratrix, referring to its use in squaring the circle [2]. While he broke the classical construction rules, this squaring of the circle was still mathematically helpful. Many such attempts resulted in the discovery of new curves. In ca. 225 B.C., Archimedes used his spiral of Archimedes in yet another method of squaring the circle [4].

### 3 Algebra Background

Abstract algebra concepts and ideas that will be needed throughout the remainder of this paper are the following: fields, field extensions, and algebraic numbers. Unless noted otherwise, the definitions in this section come from Durbin's book *Modern Algebra* [3].

#### 3.1 Rings and Fields

**Definition 3.** A ring is a set  $R$  together with two operations on  $R$ , called **addition** ( $a + b$ ) and **multiplication** ( $ab$ ) such that

- i)  $R$  with addition is an Abelian group,
- ii)  $R$  with multiplication is associative, and
- iii)  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$  for all  $a, b, c \in R$ .

An example of a ring is the set  $\mathbb{Z}$  of integers. The integers form an Abelian group under addition, and satisfy both associativity and commutativity under multiplication.

**Definition 4.** A commutative ring in which the set of nonzero elements forms a group with respect to multiplication is called a **field**.

Some examples of fields include the set  $\mathbb{Q}$  of rational numbers, or the set  $\mathbb{R}$  of real numbers. The set  $\mathbb{Z}$  of integers however is not a field, since it lacks multiplicative inverses, i.e. fractions.

#### 3.2 Polynomials

**Definition 5.** If  $R$  is a commutative ring, and  $a_0, a_1, \dots, a_n \in R$ , then an expression of the form

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

is called a **polynomial in  $x$** . The set of all polynomials in  $x$  over  $R$  is denoted  $R[x]$ .

So, for example,  $\mathbb{Z}[x]$  would be the set of all polynomials with integer coefficients. This would include such polynomials as  $f(x) = x^3 - 9x^2 + 543x + 900 - 2$ ,  $g(x) = 5$ , and  $h(x) = 8x^43$ .

The following two definitions are restricted in generality for the purposes of this paper. The notation used comes from the book *Abstract Algebra and Famous Impossibilities* [1].

**Definition 6.** The *irreducible polynomial* of  $\alpha$ , written  $\text{irr}(\alpha, \mathbb{Q})$ , is the unique, irreducible, monic polynomial  $f(x) \in \mathbb{Q}[x]$  of least degree such that  $f(\alpha) = 0$ .

For example, the irreducible polynomial of  $\sqrt{2}$  is  $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ .

**Definition 7.** The *degree* of  $\alpha$ , written  $\deg(\alpha, \mathbb{Q})$ , is the degree of the polynomial  $\text{irr}(\alpha, \mathbb{Q})$ .

For the previous example, the degree of  $\sqrt{2}$  would be  $\deg(\sqrt{2}, \mathbb{Q}) = 2$ .

### 3.3 Extension Fields

**Definition 8.** If  $E$  and  $F$  are fields, then  $E$  is said to be an *extension field* of  $F$  if  $E$  contains a subfield isomorphic to  $F$ .

The set  $\mathbb{R}$  of real numbers is an extension field of the set  $\mathbb{Q}$  of rational numbers.

### 3.4 Algebraic Numbers

**Definition 9.** Assume that  $E$  is an extension field of  $F$ . An element  $\alpha \in E$  is said to be *algebraic* over  $F$  if  $\alpha$  is a solution of some polynomial equation with coefficients in  $F$ . If an element in  $E$  is not algebraic over  $F$ , then it is called *transcendental*.

For example, the number 17 is algebraic over  $\mathbb{Q}$  as it is the solution of the polynomial  $x - 17 = 0$ . In this case 17 is algebraic over  $\mathbb{Q}$  and is also an element of  $\mathbb{Q}$ . However, the number  $\sqrt[3]{2}$  is also algebraic over  $\mathbb{Q}$ , as it is an element of an extension field of  $\mathbb{Q}$  and is a solution of the polynomial equation  $x^3 - 2 = 0$ .

## 4 Constructible Numbers

With this algebra background, we can now present some theorems concerning constructible numbers. Recall from Definition 1 that the set of constructible numbers consists of all the lengths of line segments one can create starting from a unit length of one. With this definition, it is fairly intuitive to see that one can add and subtract numbers—one simply copies the length of the segment to add or subtract onto the existing segment. Thus the set of integers is a subset of the set of constructible numbers. It can also be shown that multiplication and division can be accomplished, hence the set of the rationals is also a subset of the set of constructible numbers.

To demonstrate multiplication, we refer to figure 11. Let  $\alpha, \beta$  be the numbers you desire to multiply. Begin with the following setup: two line segments of length  $\alpha, \beta$  respectively, and an angle with vertex point  $O$ .

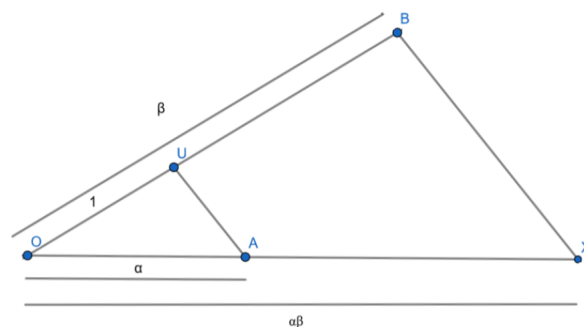


Figure 11: Multiplication

Mark points  $A$  and  $B$  on the angle, so that  $\overline{OA}$  is length  $\alpha$  and  $\overline{OB}$  is length  $\beta$ . Mark point  $U$  on  $\overrightarrow{OB}$  so that  $\overline{OU}$  is length one. Connect  $U, A$  to form a line segment  $\overline{UA}$ . Then, through  $B$ , construct a line segment parallel to  $\overline{UA}$ , and mark where it intersects  $\overrightarrow{OA}$  as point  $X$ . Now, as  $\overline{UA} \parallel \overline{BX}$ ,  $\angle OUA \cong \angle OBX$ , and  $\angle OAU \cong \angle OXB$ . Furthermore,  $\angle UOA = \angle BOX$ . Thus,  $\triangle OUA \sim \triangle OBX$ . As the sides of similar triangles are in proportion to each other, we get that

$$\frac{OX}{OA} = \frac{OB}{OU}.$$

We know that  $OA = \alpha$ ,  $OB = \beta$ , and  $OU = 1$ . Thus

$$\frac{OX}{\alpha} = \frac{\beta}{1},$$

and solving for  $OX$  we get

$$OX = \alpha\beta.$$

The idea for division is quite similar, also involving the use of similar triangles.

With the operations of addition, subtraction, multiplication, and division now apparent, it follows that the set of all constructible numbers forms a field.

**Theorem 10.** *The set of all constructible numbers forms a field.*

*Proof.* As shown above, we can perform addition, subtraction, multiplication, and division. As the set of the constructible numbers is a subset of the reals, it follows that we have associativity and commutativity under both addition and multiplication. Hence, the set of constructible numbers is a subset of the set  $\mathbb{R}$  of real numbers. ■

In addition to the field operations of addition, subtraction, multiplication, and division, we can also construct line segments with length the square root of any constructible number.

Figure 12 visualises the construction of square roots. Begin with two line segments of length 1 and  $\alpha$ , and a line with point  $O$  marked on it. Copy the length

$\alpha$  onto the line, creating line segment  $\overline{OA}$ , so the length of  $\overline{OA}$  is  $\alpha$ . Copy the segment of length 1 to create line segment  $\overline{UO}$ , with  $\overline{UO}$  having length 1. Bisect  $\overline{UA}$  to create point  $M$ , and then draw a semi-circle with center  $M$  and radius  $MA$ . Draw a line through  $O$  perpendicular to  $\overline{UA}$ , and let  $X$  be the point where this line intersects the semi-circle.

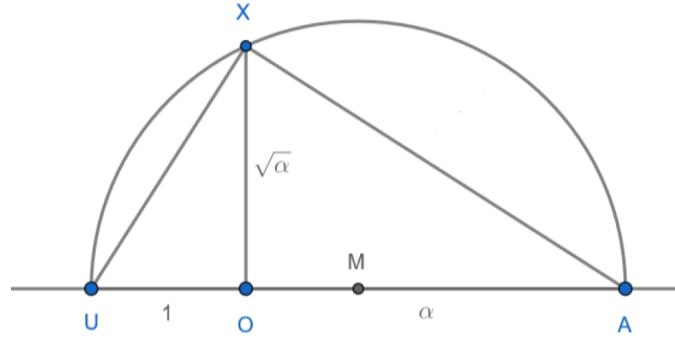


Figure 12: Square Root

As  $\triangle XUA$  is inscribed in a semi-circle, it follows that  $\angle UXA = 90^\circ$ . Thus, as  $\triangle UOX$  and  $\triangle XUA$  are both right triangles, and it follows that  $\angle OXU \cong \angle UAX = \angle OAX$ .

Now consider the right triangles  $\triangle UOX$  and  $\triangle XOA$ . As  $\angle UOX \cong \angle XOA$  and  $\angle OXU \cong \angle OAX$ ,  $\triangle UOX \sim \triangle XOA$  by definition of similar triangles. As the sides of similar triangles are in proportion to each other, it follows that

$$\frac{OX}{UO} = \frac{OA}{OX}.$$

We know that  $OA = \alpha$ , and  $UO = 1$ . Thus

$$\frac{OX}{1} = \frac{\alpha}{OX},$$

and solving for  $OX$  we get

$$(OX)^2 = \alpha, \quad OX = \sqrt{\alpha}.$$

#### 4.1 Two Important Theorems

With these preliminaries, we are finally ready state two important theorems. The first one concerns constructible numbers.

**Theorem 11** (All Constructibles Come From Square Roots). *A real number  $\gamma$  is constructible if and only if there exist positive real numbers  $\gamma_1, \gamma_2, \dots, \gamma_n$  such that*

$$\begin{aligned} \gamma_1 &\in \mathbb{F}_1 \text{ where } \mathbb{F}_1 = \mathbb{Q}, \\ \gamma_2 &\in \mathbb{F}_2 \text{ where } \mathbb{F}_2 = \mathbb{F}_1(\sqrt{\gamma_1}), \\ &\vdots \\ \gamma_n &\in \mathbb{F}_n \text{ where } \mathbb{F}_n = \mathbb{F}_{n-1}(\sqrt{\gamma_{n-1}}), \\ &\text{and} \\ \gamma &\in \mathbb{F}_{n+1} \text{ where } \mathbb{F}_{n+1} = \mathbb{F}_n(\sqrt{\gamma_n}). \end{aligned}$$

*Proof.* ( $\Rightarrow$ ) When intersecting lines, circles, or a circle and line to get new points, the worst that can happen is the need to create more square roots. Assume  $\gamma$  is constructible, so a line segment of length  $|\gamma|$  can be constructed. By Definition 1, a real number  $\gamma$  is constructible if, starting with two points  $P_1, P_2$  one unit length apart and doing a finite number of the above two methods of creating new points, we can create new points  $P_i, P_j$  such that the length of  $\overline{P_i P_j}$  is  $|\gamma|$  units.

To find the length of this line segment, we need the coordinates of each of the endpoints. These can be found in cases, as by the rules of construction each endpoint is formed by either the intersection of two lines, a line and a circle, or two circles.

i) For the intersection of two lines, let the equations of the lines be  $ax + by + c = 0$  and  $dx + ey + f = 0$  respectively, where  $a, b, c, d, e, f$  are constructible numbers. Then  $x, y$  are found by solving the two simultaneous linear equations, something that can be accomplished using only field operations, so the coordinates of the intersection point is also a constructible number as the set of all constructible numbers forms a field.

ii) For the intersection of a line and a circle, let the equations of the line and circle be  $ax + by + c = 0$  and  $x^2 + y^2 + dx + ey + f = 0$  respectively, again with  $a, b, c, d, e, f \in \mathbb{F}$  constructible numbers where  $\mathbb{F}$  is a field. Then we can solve the quadratic equation for  $x$ , and then substitute into the linear equation to get  $y$ . At most, this will introduce square roots, so we can get that the coordinates are either in  $\mathbb{F}$  or in a quadratic extension field of  $\mathbb{F}$ . In either case, the intersection point is constructible as we can take a square root of an element in  $\mathbb{F}$  and multiply it through to obtain the extension field.

iii) For the intersection of two circles, let the equations be  $x^2 + y^2 + ax + by + c = 0$  and  $x^2 + y^2 + dx + ey + f = 0$ . Then these two circles meet at the intersection of the first circle  $x^2 + y^2 + ax + by + c = 0$  and the line  $(a - d)x + (b - e)y + (c - f) = 0$ . Now, we have the form of a line and a circle intersecting, so the conclusion is the same as before.

Now, the distance between two constructible numbers will be constructible, as the set of constructible numbers forms a field and we can perform square root operations. Applying the distance formula to the constructible endpoint coordinates gives the length  $|\gamma|$  in terms of rationals and square roots. Thus we can build

the tower of fields as desired.

( $\Leftarrow$ ) Assume there exists positive real numbers  $\gamma_1, \gamma_2, \dots, \gamma_n$  such that the tower of fields listed in the theorem holds. As each field extension is done by adjoining a square root starting with the constructible field of the rationals, this is constructible as we can take successive square roots to adjoin to each field. Thus,  $\gamma$  is constructible. ■

With this theorem proven, the following are some examples of constructible numbers:  $5, \frac{3}{4}, \frac{2}{3} + \sqrt{8}, \sqrt{\frac{3}{8} + \sqrt{2}}$ , and  $\frac{5}{8}\sqrt{3} + \frac{\sqrt{7-2\sqrt{3}}}{1-\sqrt{3}}$ . Thus, even though a number may look complicated, a line segment of its length can still potentially be constructed with straight edge and compass.

That all constructible numbers come from square roots lays the foundation for the next theorem, which is key for proving the impossibility of the three Greek constructions.

**Theorem 12.** *If a real number  $\gamma$  is constructible, then  $\deg(\gamma, \mathbb{Q}) = 2^s$  for some integer  $s \geq 0$ , and  $\gamma$  is algebraic.*

*Proof.* Let  $\gamma \in \mathbb{R}$  be constructible, and let  $\gamma_1, \gamma_2 \dots \gamma_n$  be as in Theorem 11. Consider  $\sqrt{\gamma_i}$ , which is a zero of the polynomial  $p(x) = x^2 - \gamma_i$ . By definition,  $p(x) \in \mathbb{F}_i[x]$  because  $\gamma_i \in \mathbb{F}_i$ . Thus,  $\deg(\sqrt{\gamma_i}, \mathbb{F}_i)$  cannot be greater than 2, so it is either 1 or 2. Now, as  $\mathbb{F}_{i+1} = \mathbb{F}_i(\sqrt{\gamma_i})$ , it follows that  $[\mathbb{F}_{i+1} : \mathbb{F}_i] = 1$  or 2. Thus, looking at the successive tower of fields, the degree of  $\gamma$  must be  $2^s$  where  $s$  is the number of times the degree of  $[\mathbb{F}_{i+1} : \mathbb{F}_i]$  equals 2.

Now, as the degree of  $\gamma$  over  $\mathbb{Q}$  is  $2^s$ , every set of  $2^s + 1$  elements must be linearly dependent over  $\mathbb{Q}$ . Consider the set  $\{1, \gamma, \gamma^2, \dots, \gamma^{2^s}\}$ . As this set has  $2^s + 1$  elements, it is linearly dependent over  $\mathbb{Q}$  and thus there exists  $c_0, c_1, \dots, c_{2^s} \in \mathbb{Q}$ , not all zero, such that  $c_0 1 + c_1 \gamma + \dots + c_{2^s} \gamma^{2^s} = 0$ . Letting  $p(x) = c_0 + c_1 x + \dots + c_{2^s} x^{2^s}$ , it follows that  $\gamma$  is a zero of  $p(x)$ . Thus  $\gamma$  is algebraic by definition. ■

## 5 Transcendence of $\pi$

To prove the impossibility of the third construction—that of squaring the circle—it first must be shown that  $\pi$  is not algebraic. This was done by Ferdinand von Lindemann in 1882 in his paper “Über die Zahl  $\pi$ ”, published in *Mathematische Annalen* [7]. The proof we will present of the fact that  $\pi$  is transcendental is an adaptation of the approach used in the book *Abstract Algebra and Famous Impossibilities* [1]. We begin with the following propositions.

**Proposition 13.** *Let  $\mathbb{F}$  be a field and let  $t(x) \in \mathbb{F}[x]$  be a polynomial of degree  $n$  with  $n$  zeros  $\alpha_1, \alpha_2, \dots, \alpha_n$  in some extension field  $\mathbb{E}$  of  $\mathbb{F}$ . Assume that  $k \in \mathbb{Z}$ ,  $1 \leq k \leq n$ , and let  $\gamma_1, \gamma_2, \dots, \gamma_m$  be all the sums of exactly  $k$  of the  $\alpha_i$ 's. Then there is a monic polynomial  $t_k(x) \in \mathbb{F}[x]$  of degree  $m$  which has  $\gamma_1, \gamma_2, \dots, \gamma_m$  as its zeros.*

*Proof.* For the proof of this proposition we refer to the book *Abstract Algebra and Famous Impossibilities* [1]. ■

For an example of the above theorem, we can consider the polynomial  $f(x) = x^3 - 3x^2 + 4x - 12 \in \mathbb{Q}[X]$ . This is a polynomial of degree 3 with three zeros:  $-\sqrt{2}, \sqrt{2}, 3$ . Thus, in this case,  $n = 3$ ,  $\alpha_1 = -\sqrt{2}, \alpha_2 = \sqrt{2}$  and  $\alpha_3 = 3$ . Consider the case of  $k = 2$ . All the possible ways to sum exactly two of the alpha's are as follows:  $\gamma_1 = \sqrt{2} - \sqrt{2} = 0, \gamma_2 = \sqrt{2} + 3, \gamma_3 = 3 - \sqrt{2}$ . Now the theorem asserts that there is a monic polynomial  $t_x(x)$  of degree three that has  $\gamma_1, \gamma_2, \gamma_3$  as its zeros. We can find this by multiplying  $(x)(x - 3 + \sqrt{2})(x - 3 - \sqrt{2})$  to get  $t_2(x) = x^3 - 6x^2 + 7x$ .

**Proposition 14.** Suppose  $\pi$  is algebraic over  $\mathbb{Q}$ . Then there exists  $m, q, b, b_0 \in \mathbb{Z}$  with  $m, q, b \geq 1$  and  $\beta_1, \beta_2, \dots, \beta_m \in \mathbb{C}$  with  $\beta_1, \beta_2, \dots, \beta_m \neq 0$  such that

$$e^{\beta_1} + e^{\beta_2} + \dots + e^{\beta_m} + q = 0 \quad (1)$$

and the polynomial

$$\begin{aligned} h(x) &= b(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m) \\ &= bx^m + b_{m-1}x^{m-1} + \dots + b_0 \end{aligned} \quad (2)$$

has integer coefficients.

*Proof.* Suppose  $\pi$  is algebraic over  $\mathbb{Q}$ . Then as  $i$  is algebraic over  $\mathbb{Q}$ , being a root of the polynomial  $f(x) = x^2 + 1$ , it follows that  $i\pi$  is also algebraic over  $\mathbb{Q}$ . Let  $t(x) = \text{irr}(i\pi, \mathbb{Q})$ , so  $t(x)$  is a monic polynomial with rational coefficients, and  $t(i\pi) = 0$ . By the Fundamental Theorem of Algebra, we can factor  $t(x)$  as

$$t(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

where  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{C}$ . As  $t(i\pi) = 0$ , one of these  $\alpha_i$ 's must equal  $i\pi$ . Without loss of generality, say  $\alpha_1 = i\pi$ . Since  $e^{i\pi} = -1$ , we have that  $(e^{i\pi} + 1) = 0$ . As  $\alpha_1 = i\pi$ ,  $(e^{\alpha_1} + 1) = 0$  and

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_k} + 1) = 0 \quad (3)$$

If we expand equation 3, we have  $2^k$  terms on the left hand side. Simplifying using the property that  $e^{z_1} e^{z_2} = e^{z_1 + z_2}$ , we get

$$e^{\gamma_1} + e^{\gamma_2} + \dots + e^{\gamma_N} + 1 = 0 \quad (4)$$

where  $N = 2^k - 1$  and  $\gamma_i$  is a sum of  $\alpha_i$ 's. Now, applying Proposition 13, we have that

$\exists$  a monic polynomial  $t_1(x) \in \mathbb{Q}[x]$  which has all the  $\alpha_i$ 's as its zeros,  
 $\exists$  a monic polynomial  $t_2(x) \in \mathbb{Q}[x]$  which has all the sums of exactly 2  $\alpha_i$ 's as its zeros,  
 ...

$\exists$  a monic polynomial  $t_k(x) \in \mathbb{Q}[x]$  which has all the sums of exactly  $k$   $\alpha_i$ 's as its zeros.

Thus, if

$$T(x) = t_1(x)t_2(x) \cdots t_k(x)$$

then  $T(x)$  is monic, has rational coefficients, and has all  $N = 2^k - 1$   $\gamma_i$ 's as its zeros and

$$T(x) = (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_N). \quad (5)$$

We note that some of the  $\gamma_i$ 's might be zero, so if there are  $q_1$   $\gamma_i$ 's equal to zero, we write equation 4 as

$$e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_m} + q = 0$$

where  $\beta_1, \beta_2, \dots, \beta_m \in \mathbb{C}, \beta_1, \beta_2, \dots, \beta_m \neq 0$  and  $q = q_1 + 1$ . As  $q \in \mathbb{Z}, q > 0$ , we have now fulfilled the requirements of (1) for this proposition.

Now, for the second part of this proposition, note that  $m \geq 1$  or else by (1),  $q = 0$  which can't be as  $q = q_1 + 1$  and  $q_1 \geq 0$ .

With the notation of  $\beta_i$ 's and  $q$  as previously, we rewrite equation 5 as

$$T(x) = x^{q-1}(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m). \quad (6)$$

Now,  $T(x)$  is a polynomial with rational coefficients,  $x^{q-1}$  has rational coefficients, so  $(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m)$  must also have rational coefficients. Letting  $h(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m)$  and multiplying by a sufficiently large  $b \in \mathbb{Z}$  to cancel out any possible denominators, we get

$$h(x) = b(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m) = bx^m + b_{m-1}x^{m-1} + \cdots + b_0. \quad (7)$$

with  $b_0 \in \mathbb{Z}$ . Thus  $h(x)$  has integer coefficients as desired.  $\blacksquare$

Proving the transcendence of  $\pi$  will require the use of multiple lemmas presented below.

**Lemma 15.** *For every  $k \in \mathbb{Z}, k \geq 0$ , there exists a polynomial  $g_k(x) \in \mathbb{R}[x]$  such that, for every  $r \in \mathbb{R}$ ,*

$$\int_0^1 (ur)^k e^{-ur} r \, du = k! - e^{-r} g_k(r) \quad (8)$$

*Proof.* The proof follows from mathematical induction and integration by parts.

For  $k = 0$ , note that

$$\int_0^1 (ur)^0 e^{-ur} r \, du = \int_0^1 e^{-ur} r \, du = -e^{-ur} \Big|_0^1 = -e^{-1r} + e^0 = 1 - e^{-r} = 0! - e^{-r}.$$

Thus, letting  $g_0(r) = 1$ , we have that (8) is true for  $k = 0$ .

Next, we assume that (8) is true for some  $k \in \mathbb{Z}, k \geq 0$ . Then, for  $k+1$ , by integration by parts we get

$$\int_0^1 (ur)^{k+1} e^{-ur} r \, du = - (ur)^{k+1} e^{-ur} \Big|_0^1 + (k+1) \int_0^1 (ur)^k e^{-ur} r \, du.$$

Simplifying and applying the induction hypothesis, we get that this is equal to

$$\begin{aligned} & -r^{k+1} e^{-r} + (k+1)(k! - e^{-r} g_k(r)) \\ & = -r^{k+1} e^{-r} + (k+1)k! - (k+1)e^{-r} g_k(r) \\ & = (k+1)! - e^{-r}(r^{k+1} + (k+1)g_k(r)). \end{aligned}$$

If we let  $r^{k+1} + (k+1)g_k(r)$  be  $g_{k+1}(r)$ , we have the desired form. Thus (8) is true for  $k+1$ , and by the principle of mathematical induction, (8) is true for all  $k \in \mathbb{Z}, k \geq 0$ .  $\blacksquare$

As an example of applying the above theorem, the case of  $k=0$  is already shown as the base step in the proof. For the case of  $k=1$ , it can be shown that  $\int_0^1 (ur)^1 e^{-ur} r \, du = 1! - e^{-r} g_1(r)$  where  $g_1(x) = x+1$ . For  $k=2$ , the resulting equation is  $\int_0^1 (ur)^2 e^{-ur} r \, du = 2! - e^{-r} g_2(r)$  where  $g_2(x) = x^2 + 2x + 1$ .

The next lemma is very similar to the previous one.

**Lemma 16.** *For every  $k \in \mathbb{Z}, k \geq 0$ , there exists a polynomial  $h_k(x) \in \mathbb{R}[x]$  such that, for every  $r \in \mathbb{R}$ ,*

$$\int_0^1 (ur-r)^k e^{-ur} r \, du = h_k(r) - e^{-r} k!. \quad (9)$$

*Proof.* For  $k=0$ , note that

$$\begin{aligned} \int_0^1 (ur-r)^0 e^{-ur} r \, du &= \int_0^1 e^{-ur} r \, du \\ &= -e^{-ur} \Big|_0^1 = -e^{-r} + e^0 \\ &= 1 - e^{-r} = 1 - e^{-r} 0!. \end{aligned}$$

Thus, letting  $h_0(r) = 1$ , we have that (9) is true for  $k=0$ .

Now, assume (9) is true for some  $k \in \mathbb{Z}, k \neq 0$ . Then, for  $k+1$ , applying integration by parts gives

$$\begin{aligned}
\int_0^1 (ur-r)^{k+1} e^{-ur} r \, du &= - (ur-r)^{k+1} e^{-ur} \Big|_0^1 + \\
&\quad \int_0^1 (k+1)(ur-r)^k e^{-ur} r \, du \\
&= (-r)^{k+1} + (k+1) \int_0^1 (ur-r)^k e^{-ur} r \, du \\
&= (-r)^{k+1} + (k+1)[h_k(r) - e^{-r}k!] \\
&= (-r)^{k+1} + (k+1)h_k(r) - e^{-r}(k+1)k! \\
&= (-r)^{k+1} + (k+1)h_k(r) - e^{-r}(k+1)!.
\end{aligned}$$

Let  $(-r)^{k+1} + (k+1)h_k(r)$  be  $h_{k+1}(r)$ . Then (9) holds for  $k+1$ . Therefore, by the principle of mathematical induction, (9) is true for all  $k \in \mathbb{Z}$ ,  $k \geq 0$ . ■

**Lemma 17.** *Given a polynomial  $f(x) \in \mathbb{R}[x]$ , there exists  $M \in \mathbb{R}$  and  $G(x) \in \mathbb{R}[x]$  such that, for every  $r \in \mathbb{C}$ ,*

$$\int_0^1 f(ur) e^{-ur} r \, du = M - e^{-r} G(r).$$

*Proof.* Let  $f(x) \in \mathbb{R}[x] = a_m x^m + \cdots + a_1 x + a_0$ . Then

$$\begin{aligned}
\int_0^1 f(ur) e^{-ur} r \, du &= \int_0^1 (a_m(ur)^m + \cdots + a_1(ur) + a_0) e^{-ur} r \, du \\
&= \int_0^1 (a_m(ur)^m e^{-ur} r + \cdots + a_1(ur) e^{-ur} r + a_0 e^{-ur} r) \, du \\
&= \int_0^1 a_m(ur)^m e^{-ur} r \, du + \cdots + \int_0^1 a_1(ur) e^{-ur} r \, du + \int_0^1 a_0 e^{-ur} r \, du \\
&= a_m \int_0^1 (ur)^m e^{-ur} r \, du + \cdots + a_1 \int_0^1 (ur) e^{-ur} r \, du + a_0 \int_0^1 e^{-ur} r \, du \\
&= a_m(m! - e^{-r} g_m(r)) + \cdots + a_1(1! - e^{-r} g_1(r)) + a_0(0! - e^{-r} g_0(r)) \\
&= (a_m m! + \cdots + a_1 1! + a_0 0!) - e^{-r} (a_m g_m(r) + \cdots + a_1 g_1(r) + a_0 g_0(r)).
\end{aligned}$$

Let

$$M = a_m m! + \cdots + a_1 1! + a_0 0! \in \mathbb{R}$$

and

$$G(x) = a_m g_m(r) + \cdots + a_1 g_1(r) + a_0 g_0(r) \in \mathbb{R}[x]$$

as each  $g_i(x) \in \mathbb{R}[x]$ . Then  $\int_0^1 f(ur) e^{-ur} r \, du = M - e^{-r} G(x)$ . ■

For an example of this lemma, consider the polynomial  $f(x) = 3x^2 - 8x + 4$ . Calculating

$$\int_0^1 f(ur)e^{-ur}r \, du = \int_0^1 (3x^2 - 8x + 4)e^{-ur}r \, du$$

gives, after simplification,  $2 - e^{-r}(3r^2 - 2r - 1)$ . Thus we have that  $M = 2$  and  $G(x) = 3x^2 - 2x - 1$ .

For the proof of the next lemma, we will need the following lemma about polynomials in the reals.

**Lemma 18.** *For  $g(x), h(x) \in \mathbb{R}[x]$ , if  $g(x) = h(x)e^{-x}$  for every  $x \in \mathbb{R}$ , then  $g(x) = h(x) = 0$ .*

*Proof.* Let  $g(x), h(x) \in \mathbb{R}[x]$  such that  $g(x) = h(x)e^{-x} \forall x \in \mathbb{R}$ . Then  $h(x) = g(x)e^x$ . Differentiating this equation gives

$$h'(x) = g(x)e^x + g'(x)e^x,$$

and multiplying by  $g(x)$  we have

$$g(x)h'(x) = e^x(g(x))^2 + e^x g(x)g'(x).$$

We know that  $h(x) = g(x)e^x$ , so by substitution

$$g(x)h'(x) = h(x)g(x) + h(x)g'(x).$$

Rearranging terms gives

$$g(x)h(x) = h'(x)g(x) - h(x)g'(x).$$

Now, note that if either  $g(x)$  or  $h(x)$  equals 0, as  $g(x) = h(x)e^x$ , it follows that  $g(x) = h(x) = 0$ . Thus, assume both  $g(x), h(x) \neq 0$ . Let the  $\deg(g(x)) = m$  and  $\deg(h(x)) = n$ , where  $m, n \neq 0$ . Then the  $\deg(g'(x)) = m - 1$  and  $\deg(h'(x)) = n - 1$ . It follows that the degree of  $g(x)h(x)$  would be  $m + n$ . The degree of  $h'(x)g(x)$  would be  $m + n - 1$ , and the degree of  $g'(x)h(x)$  would also be  $m + n - 1$ , so the degree of  $h'(x)g(x) - g'(x)h(x)$  would be  $\leq m + n - 1$ . Now,  $g(x)h(x) = h'(x)g(x) - g'(x)h(x)$  so the degrees of these two polynomials should be equal, but  $m + n > m + n - 1$ . This is a contradiction, so the assumption that  $g(x), h(x) \neq 0$  is false and thus  $h(x) = g(x) = 0$ . ■

**Lemma 19.**  *$M$  and  $G(x)$  as in Lemma 17 are unique in the sense that, if  $p_1(x), p_2(x) \in \mathbb{R}[x]$  such that*

$$\int_0^1 f(ur)e^{-ur}r \, du = p_1(r) - e^{-r}p_2(r)$$

*for every  $r \in \mathbb{C}$ , then  $p_2(x) = G(x)$  and  $p_1(x) = M$  (a constant).*

*Proof.* Assume that  $\forall r \in \mathbb{C}$

$$\int_0^1 f(ur)e^{-ur}r \, du = p_1(r) - e^{-r}p_2(r).$$

By Lemma 17, we know that

$$\int_0^1 f(ur)e^{-ur}r \, du = M - e^{-r}G(r)$$

for some  $M \in \mathbb{R}$  and  $G(x) \in \mathbb{R}[x]$ . Thus,

$$M - e^{-r}G(r) = p_1(r) - e^{-r}p_2(r)$$

and

$$M - p_1(r) = e^{-r}(G(r) - p_2(r)).$$

Now  $M - p_1(x)$  and  $G(x) - p_2(x)$  are both polynomials over the reals, so by Lemma 18, each polynomial is equal to 0. Thus,

$$M = p_1(x)$$

and

$$G(x) = p_2(x).$$

■

With these lemmas completed, we are now ready to state a definition.

**Definition 20.** Let

$$f(x) = \frac{x^{p-1}(h(x))^p}{(p-1)!} \quad (10)$$

where the polynomial  $h(x)$  is given by (2) and (7), and  $p$  is prime,  $p > q, b, |b_0|$ , with  $q, b, |b_0|$  as in Proposition 14. Let  $n = mp + p - 1$ , so  $n = \deg f(x)$ . Let  $M, G(x)$  be as in Lemma 17. For  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ , we define

$$M_r = b^n G(r)$$

and

$$\varepsilon_r = b^n e^r \int_0^1 f(ur)e^{-ur}r \, du.$$

Now, we need still more lemmas.

**Lemma 21.**  $M$  from Lemma 17 is an integer which does not have  $p$  as a factor when  $p > |b_0|$  where  $b_0$  is as in (7).

*Proof.* From (10), we have that

$$f(x) = \frac{x^{p-1}(h(x))^p}{(p-1)!}.$$

Using equation 7,

$$f(x) = \frac{1}{(p-1)!} x^{p-1} (bx^m + b_{m-1}x^{m-1} + \cdots + b_0)^p$$

Expanding  $f(x)$  in powers of  $x$ , we can rewrite  $f(x)$  as

$$f(x) = \frac{1}{(p-1)!} (a_{p-1}x^{p-1} + a_px^p + \cdots + a_nx^n) \quad (11)$$

where  $a_{p-1}, \dots, a_n \in \mathbb{Z}$  and  $a_{p-1} = b_0^p \neq 0$ .

Now consider  $\int_0^1 f(ur)e^{-ur}r \, du$ . Substituting (11) for  $f(x)$ , we get

$$\begin{aligned} & \int_0^1 f(ur)e^{-ur}r \, du \\ &= \int_0^1 \frac{1}{(p-1)!} (a_{p-1}(ur)^{p-1} + a_p(ur)^p + \cdots + a_n(ur)^n) e^{-ur}r \, du. \end{aligned}$$

By linearity of integration, we have

$$= \frac{1}{(p-1)!} \left( a_{p-1} \int_0^1 (ur)^{p-1} e^{-ur}r \, du + \cdots + a_n \int_0^1 (ur)^n e^{-ur}r \, du \right).$$

Applying Lemma 15 yields

$$= \frac{1}{(p-1)!} (a_{p-1}(p-1)! + a_pp! + \cdots + a_nn!) - e^{-r}(\text{some polynomial})$$

By Lemma 19 concerning uniqueness, we conclude that

$$\begin{aligned} M &= \frac{1}{(p-1)!} (a_{p-1}(p-1)! + a_pp! + \cdots + a_nn!) \\ &= a_{p-1} + a_pp + \cdots + a_n(n(n-1) \cdots (p+1)p). \end{aligned}$$

As  $a_i, p, n \in \mathbb{Z}$ , we have that  $M \in \mathbb{Z}$ . Also, it is obvious that  $p$  is a factor of each term of  $M$  except possibly  $a_{p-1}$ . To show that  $p$  is not a factor of  $M$ , recall that  $a_{p-1} = b_0^p$ . Now, as each  $\beta_i \neq 0$  from Proposition 14, it follows that  $b_0 \neq 0$ . Since  $p$  is prime, when  $p > |b_0|$  it follows that  $p$  cannot divide  $b_0$  and thus cannot divide  $b_0^p$ . ■

Now we will manipulate  $f(x)$  and prove another lemma. We expand  $f(x)$  from equation 10 in powers of  $(x-r)$ ,  $r \in \mathbb{C}$ . Then,

$$f(x) = \frac{1}{(p-1)!} (d_0(r) + d_1(r)(x-r) + \cdots + d_n(r)(x-r)^n) \quad (12)$$

where  $d_0(x), d_1(x), \dots, d_n(x) \in \mathbb{Z}[x]$ .

**Lemma 22.** *With notation as in (12), if  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$  then  $d_0(r) = d_1(r) = \cdots = d_{p-1}(r) = 0$ .*

*Proof.* By definition of  $h(x)$  in (7), it follows that  $(x-r)^p$  is a factor of  $h(x)^p$ . Thus we can write  $f(x) = \frac{1}{(p-1)!} (x-r)^p g(x)$  for some  $g(x)$ . Expanding this  $g(x)$  in powers of  $(x-r)$  and multiplying through, we get

$$f(x) = \frac{1}{(p-1)!} (b_p(x-r)^p + b_{p+1}(x-r)^{p+1} + \cdots + b_n(x-r)^n). \quad (13)$$

Note that  $n > p$  by definition of  $n$ . Now we equate coefficients from equations (13) and (12). It follows that all the coefficients on  $(x-r)^{\text{less than } p \text{ power}}$  are zero. ■

With Lemma 22, we are ready to prove the following.

**Lemma 23.** *There exists a polynomial  $G_1 \in \mathbb{Z}[x]$  of degree at most  $n$  such that  $G(r) = pG_1(r), \forall r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ , where the  $\beta_i$ 's are as in Proposition 14.*

*Proof.* Using equation (12),

$$\begin{aligned} & \int_0^1 f(ur) e^{-ur} r \, du \\ &= \int_0^1 \frac{1}{(p-1)!} (d_0(r) + d_1(r)(ur-r) + \cdots + d_n(r)(ur-r)^n) e^{-ur} r \, du \\ &= \frac{1}{(p-1)!} \left( d_0(r) \int_0^1 e^{-ur} r \, du + d_1(r) \int_0^1 (ur-r) e^{-ur} r \, du + \cdots \right. \\ & \quad \left. + d_n(r) \int_0^1 (ur-r)^n e^{-ur} r \, du \right). \end{aligned}$$

Applying Lemma 16, it follows that this is a difference of two terms, where the second term is

$$\frac{e^{-r}}{(p-1)!} (d_0(r) + d_1(r)1! + \cdots + d_p(r)p! + \cdots + d_n(r)n!).$$

From Lemma 19 concerning uniqueness, we have that

$$G(r) = \frac{1}{(p-1)!} (d_0(r) + d_1(r)1! + \cdots + d_n(r)n!).$$

From Lemma 22, when  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ , we know that  $d_0(r) = d_1(r) = \dots = d_{p-1}(r) = 0$ . Thus,

$$G(r) = \frac{1}{(p-1)!} (d_p(r)p! + \dots + d_n(r)n!).$$

Distributing the  $\frac{1}{(p-1)!}$  factor, we have

$$G(r) = \frac{1}{(p-1)!} d_p(r)p! + \dots + \frac{1}{(p-1)!} d_n(r)n!.$$

Factoring out the  $p$  term yields

$$G(r) = p \left( d_p(r) + d_{p+1}(r)(p+1) + \dots + d_n(r)((n)(n-1) \dots (p+1)) \right).$$

Letting

$$G_1(x) = d_p(x) + d_{p+1}(x)(p+1) + \dots + d_n(x) \left( (n)(n-1) \dots (p+1) \right)$$

we have

$$G(r) = pG_1(r)$$

Now, as all the  $d_i(x) \in \mathbb{Z}[x]$  and are of degree at most  $n$ ,  $G_1(x)$  is also of degree at most  $n$ . ■

**Lemma 24.** Let  $f(x)$  and  $n$  be as given in Definition 20. For  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ , let  $\varepsilon_r$  be as given by Definition 20, so  $\varepsilon_r = b^n e^r \int_0^1 f(ur) e^{-ur} r du$ . Then  $\lim_{p \rightarrow \infty} \varepsilon_r = 0$ .

*Proof.* Let  $u \in [0, 1]$ ,  $x = ur$ ,  $r = r_1 + ir_2$ ,  $r_1, r_2 \in \mathbb{R}$ . We know that  $e^r = e^{r_1}(\cos(r_2) + i\sin(r_2))$ . Thus,  $|e^r| = e^{r_1}$ , and  $|e^{-ur}| = e^{-ur_1} \leq e^{|r_1|}$ . From (10) and (2), we get that

$$|f(x)| = \left| \frac{x^{p-1}}{(p-1)!} b^p (x - \beta_1)^p (x - \beta_2)^p \dots (x - \beta_m)^p \right|.$$

Thus,

$$\begin{aligned} |f(x)| &= \left| \frac{x^{p-1}}{(p-1)!} b^p (x - \beta_1)^p \dots (x - \beta_m)^p \right| \\ &\leq \frac{|r|^{p-1}}{(p-1)!} b^p (|r| + |\beta_1|)^p (|r| + |\beta_2|)^p \dots (|r| + |\beta_m|)^p. \end{aligned}$$

Note that 1 is the length of the interval of integration and

$$\frac{|r|^{p-1}}{(p-1)!} b^p (|r| + |\beta_1|)^p (|r| + |\beta_2|)^p \dots (|r| + |\beta_m|)^p e^{-ur} r$$

is an upper bound for  $|f(ur)e^{-ur}r|$ .

It can be shown [1] that an upper bound for the modulus of an integral  $\left| \int_a^b f(x) dx \right|$  when  $|f(x)| \leq c \forall x \in [a, b]$  is the following:

$$\left| \int_a^b f(x) dx \right| \leq 2c(b-a).$$

Thus,

$$\begin{aligned} & b^n e^r \int_0^1 |f(ur) e^{-ur} r| du \\ & \leq b^n e^r * 2 * \frac{|r|^{p-1}}{(p-1)!} b^p (|r| + |\beta_1|)^p (|r| + |\beta_2|)^p \cdots (|r| + |\beta_m|)^p |e^{-ur} r|. \end{aligned}$$

As  $n = mp + p - 1$ ,  $|e^r| = e^{r_1}$ , and  $|e^{-ur}| \leq e^{|r_1|}$ , we have

$$\begin{aligned} & b^n e^r \int_0^1 |f(ur) e^{-ur} r| du \\ & \leq b^{mp+p-1} e^{r_1} * 2 * \frac{|r|^{p-1}}{(p-1)!} b^p (|r| + |\beta_1|)^p (|r| + |\beta_2|)^p \cdots \\ & \quad (|r| + |\beta_m|)^p e^{|r_1|} |r| \\ & \leq \frac{C^p}{(p-1)!} 2e^{r_1} e^{|r_1|}, \end{aligned}$$

where  $C = b^{m+2} |r| (|r| + |\beta_1|) (|r| + |\beta_2|) \cdots (|r| + |\beta_m|)$ .

Note that  $C$  is independent of  $p$ . Thus, if we can show that  $\frac{C^p}{(p-1)!} \rightarrow 0$  as  $p \rightarrow \infty$ , we would have the desired result. To that end, let  $m \in \mathbb{Z}, m > 1, m \geq 2C$ . Then, for every  $p \geq m$ , we have

$$\begin{aligned} \frac{C^p}{(p-1)!} &= \frac{C}{1} \frac{C}{2} \frac{C}{3} \cdots \frac{C}{(m-1)} \frac{C}{m} \cdots \frac{C}{(p-1)} C \\ &\leq \frac{C}{1} \frac{C}{2} \frac{C}{3} \cdots \frac{C}{(m-1)} \frac{1}{2} \frac{1}{2} \cdots C = \frac{d}{2^{p-m}} \end{aligned}$$

where  $d = \frac{C}{1} \frac{C}{2} \frac{C}{3} \cdots \frac{C}{(m-1)} C$ . Thus,

$$\frac{C^p}{(p-1)!} \leq \frac{d}{2^{p-m}}$$

and

$$\lim_{p \rightarrow \infty} \frac{d}{2^{p-m}} = 0$$

so

$$\lim_{p \rightarrow \infty} \frac{C^p}{(p-1)!} = 0.$$

As

$$b^n e^r \int_0^1 |f(ur) e^{-ur} r| du \leq \frac{C^p}{(p-1)!} = 0$$

we have

$$\lim_{p \rightarrow \infty} \varepsilon_r = 0.$$

■

With the help of all these lemmas, the actual proof of  $\pi$  being transcendental is rather straightforward.

**Theorem 25.**  $\pi$  is transcendental.

*Proof.* Suppose  $\pi$  is algebraic. Let  $p$  be prime,  $p > q, b, |b_0|$  where  $q, b, b_0$  are as in Proposition 14. Let  $f(x)$  and  $n$  be as defined in Definition 20.

By Lemma 21, we have that  $\exists M \in \mathbb{Z}$  such that  $p$  does not divide  $M$ , and  $\exists G_1(x) \in \mathbb{Z}[x]$  of degree at most  $n$  such that, for  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ ,

$$\int_0^1 f(ur) e^{-ur} r du = M - e^{-r} p G_1(r). \quad (14)$$

For every  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ , let  $M, M_r, \varepsilon_r$  be as in Definition 20. By the uniqueness of Lemma 23, we get that

$$M_r = p b^n G_1(r). \quad (15)$$

Recall that

$$\varepsilon_r = b^n e^r \int_0^1 f(ur) e^{-ur} r du. \quad (16)$$

Thus,

$$M_r + \varepsilon_r = p b^n G_1(r) + b^n e^r (M - e^{-r} p G_1(r))$$

which simplifies to

$$M_r + \varepsilon_r = b^n e^r M.$$

Solving for  $e^r$ , we get

$$e^r = \frac{M_r + \varepsilon_r}{M b^n} \quad (17)$$

for  $r \in \{\beta_1, \beta_2, \dots, \beta_m\}$ .

By working with symmetric polynomials, it can be shown that  $M_{\beta_1} + M_{\beta_2} + \dots + M_{\beta_m}$  is an integer which is divisible by  $p$  [1].

Substituting (17) into (1), gives

$$[q M b^n + M_{\beta_1} + \dots + M_{\beta_m}] + [\varepsilon_{\beta_1} + \dots + \varepsilon_{\beta_m}] = 0. \quad (18)$$

Now, since  $M \in \mathbb{Z}$  and  $p$  is prime, as  $p$  does not divide  $M$ , and  $p > q, |b|$ , we have  $p$  does not divide  $q M b^n$ . Thus  $p$  does not divide  $q M b^n + M_{\beta_1} + \dots + M_{\beta_m}$ , so  $q M b^n + M_{\beta_1} + \dots + M_{\beta_m}$  must be a non-zero integer as  $p$  divides 0. Now, by Lemma 24, each of the  $\varepsilon_i$  terms can be made arbitrarily small as their limit goes

to zero when  $p$  goes to infinity. Let  $p$  be such that  $|\varepsilon_{\beta_1} + \cdots + \varepsilon_{\beta_m}| < \frac{1}{2}$ . Then we have from (18) that a non-zero integer added to a number less than  $\frac{1}{2}$  gives zero, which is a contradiction. Therefore  $\pi$  is transcendental. ■

## 6 Impossibility Proofs

With all these preliminaries, we are finally ready to present proofs of the impossibility of the three constructions.

This impossibility of doubling the cube and trisecting an arbitrary angle was first done by Pierre Wantzel in 1837 in his paper “Recherches sur les moyens de reconnaître si un problème de Géométrie peut se résoudre avec la règle et le compas” published in the Journal de Mathématiques Pures et Appliquées [8]. In 1882, Lindemann’s proof of the transcendence of  $\pi$  provided the missing piece to the proof of the impossibility of squaring the circle, and thus all three constructions were proven to be impossible.

### 6.1 Doubling the Cube

**Theorem 26.** *The cube cannot be doubled.*

*Proof.* Suppose to the contrary that the cube can be doubled. Then the basic cube of volume 1 can be doubled, creating a cube with volume 2 and thus sides of length  $\sqrt[3]{2}$ . Thus  $\sqrt[3]{2}$  must be a constructible number. We know that the irreducible polynomial of  $\sqrt[3]{2}$  over  $\mathbb{Q}$  is  $\text{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ . It follows from this that  $\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$ . Here we encounter a problem, in that  $3 \neq 2^s$  for  $s \in \mathbb{Z}, s \geq 0$ . This is a contradiction to Theorem 12, and thus our original assumption that  $\sqrt[3]{2}$  is constructible must be false. Therefore the cube cannot be doubled. ■

### 6.2 Trisecting an Arbitrary Angle

The proof of the next theorem concerning the impossibility of trisecting an arbitrary angle is similar to the one for the cube.

**Theorem 27.** *There exists an angle that cannot be trisected with only unmarked straightedge and compass.*

*Proof.* Like the proof of Theorem 26, assume by way of contradiction that every angle can be trisected with only unmarked straightedge and compass. Then, an angle of  $60^\circ$  can be trisected. From this trisected angle, one can drop a perpendicular to create a triangle. Then, as  $\cos(\theta) = \frac{\text{adjacent}}{\text{hypotenuse}}$ , it follows that a line segment of length  $\cos(20^\circ)$  can be constructed. Now, consider the trigonometric identity  $\cos(3\theta) = -3 \cos(\theta) + 4 \cos^3(\theta)$ . From this, it follows that

$$0.5 = \cos(60^\circ) = -3 \cos(20^\circ) + 4 \cos^3(20^\circ).$$

Thus, multiplying by two and rearranging terms we have

$$8 \cos^3(20^\circ) - 6 \cos(20^\circ) - 1 = 0$$

and it follows that  $\cos(20^\circ)$  is a zero of the polynomial  $p(x) = x^3 - \frac{6}{8}x - \frac{1}{8}$ . This polynomial is irreducible over  $\mathbb{Q}$ , thus  $\deg(\cos(20^\circ), \mathbb{Q}) = 3$ . This leads to the same contradiction as before in that  $3 \neq 2^s$  for  $s \in \mathbb{Z}, s \geq 0$ . Therefore by Theorem 12,  $\cos(20^\circ)$  is not constructible. Thus, it is impossible to trisect a  $60^\circ$  angle, and as there exists at least one angle which is impossible to trisect, the statement that every angle can be trisected with only unmarked straightedge and compass is false. ■

### 6.3 Squaring the Circle

Using the fact that  $\pi$  is a non-algebraic number, one can show the impossibility of squaring the circle.

**Theorem 28.** *The circle cannot be squared.*

*Proof.* Suppose by way of contradiction that the circle can be squared. Then a circle of radius 1 and area  $\pi r^2 = \pi$  can be squared, resulting in a square of area  $\pi$ . It follows that this square must have sides of length  $\sqrt{\pi}$ , so  $\sqrt{\pi}$  must be a constructible number. Since the set of constructible numbers forms a field (Lemma 10), it is closed under multiplication and thus  $\sqrt{\pi} * \sqrt{\pi} = \pi$  must also be a constructible number. Applying Lemma 12, we get that  $\pi$  is algebraic. However, by Theorem 25,  $\pi$  is transcendental, and thus is not algebraic. This is a contradiction, and therefore the circle cannot be squared. ■

### References

- [1] K. Pearson A. Jones, S. Morris, *Abstract algebra and famous impossibilities*, 1991.
- [2] Uta C. Merzbach Carl B. Boyer, *A history of mathematics*, 2nd ed., 1989.
- [3] John R. Durbin, *Modern algebra: An introduction*, 6th ed., 2009.
- [4] Howard Eves, *An introduction to the history of mathematics*, 6th ed., 1990.
- [5] Charles Robert Hadlock, *Field theory and its classical problems*, 1978.
- [6] Gerard A. Venema, *Foundations of geometry*, 2nd. ed., 2012.
- [7] Ferdinand von Lindemann, *Über die zahl  $\pi$* , *Mathematische Annalen* **20** (1882), 213–225.
- [8] Pierre Wantzel, *Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas*, *Journal de Mathématiques Pures et Appliquées* **2** (1837), 366–372.

## *The Problem Corner*

Edited by Pat Costello

*The Problem Corner* invites questions of interest to undergraduate students. As a rule, the solution should not demand any tools beyond calculus and linear algebra. Although new problems are preferred, old ones of particular interest or charm are welcome, provided the source is given. Solutions should accompany problems submitted for publication. Solutions of the following new problems should be submitted on separate sheets before July 31, 2023. Solutions received after this will be considered up to the time when copy is prepared for publication. The solutions received will be published in the Spring 2023 issue of *The Pentagon*. Preference will be given to correct student solutions. Affirmation of student status and school should be included with solutions. New problems and solutions to problems in this issue should be sent to Pat Costello, Department of Mathematics and Statistics, Eastern Kentucky University, 521 Lancaster Avenue, Richmond, KY 40475-3102 (e-mail: pat.costello@eku.edu, fax: (859) 622-3051)

### NEW PROBLEMS 901 - 910

**Problem 901.** *Proposed by José Luis Díaz-Barrero, School of Civil Engineering, Barcelona Tech - UPC, Barcelona, Spain.*

Suppose for some integer  $k \geq 2$  that  $a_1 < a_2 < \dots < a_k$  are positive integers, and that  $A$  is their least common multiple. Prove that

$$a_1a_2 + a_2a_3 + \dots + a_{k-1}a_k + a_ka_1 \leq A^2.$$

**Problem 902.** *Proposed by Daniel Sitaru, "Theodor Costescu" National Economic College, Drobeta Turnu – Severin, Mehedinti, Romania.*

Without a computer, find  $\Omega = \int_0^{\pi/30} \frac{\sin 5x \sin 7x \sin 8x}{\cos 2x \cos 3x \cos 5x \cos 10x} dx$ .

**Problem 903.** *Proposed by Daniel Sitaru, "Theodor Costescu" National Economic College, Drobeta Turnu – Severin, Mehedinti, Romania.*

Solve for complex numbers:

$$\begin{vmatrix} x^2 & x^2 + 3x & x^2 + 6x + 9 \\ x^2 + 2x + 1 & x^2 + 5x + 4 & x^2 + 8x + 16 \\ x^4 + 2x^2 + 1 & x^4 + 3x^2 + 2 & x^4 + 4x^2 + 4 \end{vmatrix} = 0.$$

**Problem 904.** *Proposed by Albert Natian, Los Angeles Valley College, Valley Glen, CA.*

Find the  $n^{\text{th}}$  term of the sequence  $(a_n)_{n \geq 0}$  defined recursively as follows:

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = 0$$

$$\forall n \geq 3: a_n = \sum_{k=1}^{n-1} (n-k)(n-k-4)a_k.$$

**Problem 905.** *Proposed by Vasile Mircea Popa, Lucian Blaga University, Sibiu, Romania.*

Calculate the following integral without a computer:

$$\int_1^{\infty} \frac{x\sqrt{x}\ln x}{(x+1)(x^2+1)} dx.$$

**Problem 906.** *Proposed by Mihaly Bencze, Braşov, Romania and Neculai Stanciu, "George Emil Palade" School, Buză, Romania.*

If  $\lambda \geq 1$  and  $ABC$  is a triangle, prove that  $\sum (\tan \frac{A}{4})^\lambda \geq 3(2 - \sqrt{3})^\lambda$ .

**Problem 907.** *Proposed by Toyesh Prakash Sharma (student), Agra College, Agra, India.*

If  $a, b, c > 0$ , then show that

$$\left(\frac{a}{b+c}\right)^{\frac{a}{b+c}} + \left(\frac{b}{c+a}\right)^{\frac{b}{c+a}} + \left(\frac{c}{a+b}\right)^{\frac{c}{a+b}} \geq 3^{\frac{2}{3}}.$$

**Problem 908.** *Proposed by Raluca Maria Caraion and Forică Anastase, "Alexandru Odobescu" High School, Lehliu-Gară, Călăraşi, Romania.*

If  $a, b, c > 0$ , then show that

$$\prod \frac{(1+ab)(1+ac)}{1+a\sqrt{bc}} \geq \left(1 + \sqrt[3]{a^2b^2c^2}\right)^3.$$

**Problem 909.** *Proposed by Seán Stewart, King Abdullah University of Science and Technology, Saudi Arabia.*

If  $m > 1$ , without a computer evaluate

$$\int_0^{\pi/2} \frac{\cot\left(\frac{x}{2}\right) \sec x \log(\cos x)}{\sqrt[m]{\sec x - 1}} dx.$$

**Problem 910.** *Proposed by the editor.*

Prove that the sum of the last two digits of  $2^n$  is never 17.

## SOLUTIONS TO PROBLEMS 881-890

**Problem 881.** *Proposed by Mathew Cropper, Eastern Kentucky University, Richmond, KY.*

Find a formula (possibly recursive) for the number of integers with  $n$  digits that contain exactly one 47 in the integer.

**Solution** *by the Ashland University Problem Solving Group, Ashland, OH.*

Let  $a_n$  be the number of  $n$ -digit integers that contain exactly one occurrence of 47, and  $b_n$  be the number of  $n$ -digit integers that contain no occurrences of 47. We first show that

$$a_n = 10(a_{n-1} - a_{n-2}) + 9a_{n-2} + b_{n-2} = 10a_{n-1} - a_{n-2} + b_{n-2}.$$

Note that  $a_{n-2}$  counts the number of  $(n-2)$ -digit numbers that contain one 47, so it also is the number of  $(n-1)$ -digit numbers that contain one 47 and end with a 4. Hence  $(a_{n-1} - a_{n-2})$  counts the number of  $(n-1)$ -digit numbers that don't end with a 4. Then we see that the formula counts the  $n$ -digit numbers with one 47 of three types: first those that have the 47 among the first  $n-1$  digits, whose next to last digit is not a four, and end with any digit. Secondly, those that have the 47 among the first  $n-2$  digits, the next to last digit is a four, and end with any digit except 7. Lastly, those that end with 47, having no 47 among the first  $n-2$  digits. Using the same reasoning, we can count the  $n$ -digit numbers with no 47 as

$$b_n = 10(b_{n-1} - b_{n-2}) + 9b_{n-2} = 10b_{n-1} - b_{n-2}.$$

Solving the  $a_n$  formula for  $b_{n-2}$  and adjusting the index on the  $b_n$  formula gives

$$\begin{aligned} b_{n-2} &= a_n - 10a_{n-1} + a_{n-2}, \\ b_{n-2} &= 10b_{n-3} - b_{n-4}. \end{aligned}$$

Now,

$$\begin{aligned} a_n - 10a_{n-1} + a_{n-2} &= 10(a_{n-1} - 10a_{n-2} + a_{n-3}) - (a_{n-2} - 10a_{n-3} + a_{n-4}) \end{aligned}$$

Solving for  $a_n$  gives the recursive formula

$$a_n = 20a_{n-1} - 102a_{n-2} + 20a_{n-3} - a_{n-4}.$$

Also solved by Avirup and Biswarup Chakraborty, Narendrapur Ramkrishna Mission Vidyalaya. Class 12; Steven Jang, Cal Poly Pomona Problem Solving Group, Pomona, CA; and the proposer.

**Problem 882.** Proposed by José Luis Díaz-Barrero, School of Civil Engineering, Barcelona Tech - UPC, Barcelona, Spain.

Find all functions  $f : \mathbb{R} \rightarrow \mathbb{R}$  that satisfy  $f(x^4 + y) = f(x) + f(y^4)$  for all  $x, y \in \mathbb{R}$ .

**Solution** by the proposer.

For  $x = y = 0$ , we have  $f(0) = f(0) + f(0) = 2f(0)$  from which  $f(0) = 0$  follows. For  $y = 0$ , we have  $f(x^4) = f(x) + f(0) = f(x)$ . Putting  $y = -x^4$ , yields

$$f(0) = f(x) + f((-x^4)^4) = f(x) + f(x^{16}) = f(x) + f(x) = 2f(x).$$

Since  $2f(x) = f(0) = 0$ , then  $f(x) = 0$  for all  $x \in \mathbb{R}$ . Thus the only function that satisfies the condition is the constant function  $f = 0$ .

Also solved by Brian Bradie, Christopher Newport University, Newport News, VA; Steven Jang, Cal Poly Pomona Problem Solving Group, Pomona, CA; and Albert Stadler, Herrliberg, Switzerland.

**Problem 883.** Proposed by Daniel Sitaru, “Theodor Costescu” National Economic College, Drobeta Turnu – Severin, Romania.

If  $a, b, c \in \mathbb{C}$  are such that  $|a^8 + 1| \leq 1$ ,  $|b^{10} + 1| \leq 1$ ,  $|c^{12} + 1| \leq 1$ ,  $|a^4 + 1| \leq 1$ ,  $|b^5 + 1| \leq 1$ , and  $|c^{16} + 1| \leq 1$ , then

$$|a + b + c| + 3 \geq |a + b| + |b + c| + |c + a|.$$

**Solution** by the proposer.

We have:

$$\begin{aligned} 2|a^8| &= |2a^8| = |(a^4 + 1)^2 - (a^8 + 1)| \\ &\leq |(a^4 + 1)^2| + |a^8 + 1| \\ &\leq |a^4 + 1|^2 + |a^8 + 1| \leq 1^2 + 1 = 2 \\ &\Rightarrow |a^8| \leq 1 \Rightarrow (|a|)^8 \leq 1 \Rightarrow |a| \leq 1; \end{aligned}$$

$$\begin{aligned} 2|b^{10}| &= |2b^{10}| = |(b^5 + 1)^2 - (b^{10} + 1)| \\ &\leq |(b^5 + 1)^2| + |b^{10} + 1| \\ &\leq |b^5 + 1|^2 + |b^{10} + 1| \leq 1^2 + 1 = 2 \\ &\Rightarrow |b^{10}| \leq 1 \Rightarrow (|b|)^{10} \leq 1 \Rightarrow |b| \leq 1; \end{aligned}$$

$$\begin{aligned}
2|c^{12}| &= |2c^{12}| = |(c^6 + 1)^2 - (c^{12} + 1)| \\
&\leq |(c^6 + 1)^2| + |c^{12} + 1| \\
&\leq |c^6 + 1|^2 + |c^{12} + 1| \leq 1^2 + 1 = 2 \\
&\Rightarrow |c^{12}| \leq 1 \Rightarrow (|c|)^{12} \leq 1 \Rightarrow |c| \leq 1.
\end{aligned}$$

We will use Hlawka's inequality for  $a, b, c \in \mathbb{C}$ :

$$|a + b + c| + |a| + |b| + |c| \geq |a + b| + |b + c| + |c + a|,$$

so

$$\begin{aligned}
|a + b + c| + 3 &= |a + b + c| + 1 + 1 + 1 \\
&\geq |a + b + c| + |a| + |b| + |c| \\
&\geq |a + b| + |b + c| + |c + a|.
\end{aligned}$$

**Problem 884.** Proposed by Daniel Sitaru, "Theodor Costescu" National Economic College, Drobeta Turnu – Severin, Romania.

If  $a, b, c > 0$  and  $a^4 + b^4 + c^4 = 3$ , then

$$\begin{aligned}
&\frac{(a^2 + b^2)^6}{(3a^8 + 10a^4b^4 + 3b^8)} + \frac{(b^2 + c^2)^6}{(3b^8 + 10b^4c^4 + 3c^8)} \\
&\quad + \frac{(c^2 + a^2)^6}{(3c^8 + 10c^4a^4 + 3a^8)} \leq 12.
\end{aligned}$$

**Solution** by Henry Ricardo, Westchester Area Math Circle, Purchase, NY.

It is easily established that

$$3a^8 + 10a^4b^4 + 3b^8 = (a^2 + b^2)^4 + 2(a^4 + b^4)(a^2 - b^2)^2 \geq (a^2 + b^2)^4$$

with equality if and only if  $a = b$ . The power mean inequality yields

$$\left(\frac{a^2 + b^2}{2}\right)^{1/2} \leq \left(\frac{a^4 + b^4}{2}\right)^{1/4} \text{ or } (a^2 + b^2)^2 \leq 2(a^4 + b^4). \text{ Combining, we see that}$$

$$\begin{aligned}
\sum_{\text{cyc}} \frac{(a^2 + b^2)^6}{3a^8 + 10a^4b^4 + 3b^8} &\leq \sum_{\text{cyc}} \frac{(a^2 + b^2)^6}{(a^2 + b^2)^4} \\
&= \sum_{\text{cyc}} (a^2 + b^2)^2 \leq 2 \sum_{\text{cyc}} (a^4 + b^4) \\
&= 4(a^4 + b^4 + c^4) = 12.
\end{aligned}$$

Also solved by Florică Anastase, “Alexandru Odobescu” High School, Lehliu-Gară, Călărași, Romania; Albert Stadler, Herrliberg, Switzerland; and the proposer.

**Problem 885.** Proposed by Dorin Marghidanu, Colegiul National ‘A. I. Cuze’, Corabia, Romania.

If  $a, b, x, y > 0$  and  $n \in \mathbb{N}^*$  prove that

$$\frac{(x+y)^n}{2^{(n-1)}} \leq \frac{(ax+by)^n + (bx+ay)^n}{(a+b)^n} \leq x^n + y^n.$$

**Solution** by Florică Anastase, “Alexandru Odobescu” High School, Lehliu-Gară, Călărași, Romania.

Let  $f : (0, 1) \rightarrow \mathbb{R}, f(t) = t^n, n \in \mathbb{N}^*$  be a convex function, then by Jensen’s inequality with weighted  $\lambda_1, \lambda_2 \in (0, 1), \lambda_1 + \lambda_2 = 1$ , we have

$$f(\lambda_1 t_1 + \lambda_2 t_2) \leq \lambda_1 f(t_1) + \lambda_2 f(t_2), \forall t_1, t_2 \in (0, \infty).$$

For  $\lambda_1 = \lambda_2 = \frac{1}{2}$  we have

$$f\left(\frac{1}{2}t_1 + \frac{1}{2}t_2\right) \leq \frac{1}{2}f(t_1) + \frac{1}{2}f(t_2). \quad (1)$$

For  $\lambda_1 = \frac{a}{a+b}, \lambda_2 = \frac{b}{a+b}$ , we have

$$f\left(\frac{a}{a+b}t_1 + \frac{b}{a+b}t_2\right) \leq \frac{a}{a+b}f(t_1) + \frac{b}{a+b}f(t_2). \quad (2)$$

Now taking  $t_1 = ax + by, t_2 = bx + ay$  in (1), it follows that

$$\begin{aligned} \frac{1}{2^n} [(ax+by) + (bx+ay)]^n &\leq \frac{1}{2} ((ax+by)^n + (bx+ay)^n) \\ \Leftrightarrow \frac{1}{2^{n-1}} (a+b)^n (x+y)^n &\leq (ax+by)^n + (bx+ay)^n \\ \Leftrightarrow \frac{(x+y)^n}{2^{n-1}} &\leq \frac{(ax+by)^n + (bx+ay)^n}{(a+b)}. \end{aligned} \quad (3)$$

Taking  $t_1 = x, t_2 = y$  in (2), it follows

$$\left(\frac{a}{a+b}x + \frac{b}{a+b}y\right)^n \leq \frac{a}{a+b}x^n + \frac{b}{a+b}y^n; \quad (4)$$

Taking  $t_1 = y, t_2 = x$  in (2), it follows

$$\left(\frac{b}{a+b}x + \frac{a}{a+b}y\right)^n \leq \frac{b}{a+b}x^n + \frac{a}{a+b}y^n. \quad (5)$$

Adding (4) and (5), we get

$$\begin{aligned} \frac{(ax+by)^n + (bx+ay)^n}{(a+b)^n} &\leq \frac{a}{a+b}x^n + \frac{b}{a+b}y^n + \frac{b}{a+b}x^n + \frac{a}{a+b}y^n \\ &\Leftrightarrow \frac{(ax+by)^n + (bx+ay)^n}{(a+b)^n} \leq x^n + y^n. \end{aligned} \quad (6)$$

From (3) and (6) we get the desired inequality.

*Also solved by Brian Bradie, Christopher Newport University, Newport News, VA; Steven Jang, Cal Poly Pomona Problem Solving Group, Pomona, CA; Angel Plaza, Universidad de Las Palmas de Gran Canaria, Spain; Henry Ricardo, Westchester Area Math Circle, Purchase, NY; Albert Stadler, Herrliberg, Switzerland; Marian Ursărescu, "Roman-Vodă" National College, Roman, Romania; and the proposer.*

**Problem 886.** *Proposed by George Stoica, Saint John, New Brunswick, Canada.* Prove that for any  $a \in (1, 2)$  and any integer  $n \geq 1$ , there exist

$$\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{-1, 1\}$$

such that

$$(a-1) \left| \varepsilon_0 + \varepsilon_1 a + \varepsilon_2 a^2 + \dots + \varepsilon_n a^n \right| < 1.$$

**Solution** *by Albert Stadler, Herrliberg, Switzerland.*

The numbers  $\varepsilon_n, \varepsilon_{n-1}, \dots, \varepsilon_0$  are determined recursively according to the following algorithm: Take  $a^n$  and subtract successively the numbers  $a^j$  with  $j < n$  until

$$a^n - a^{n-1} - a^{n-2} - \dots - a^{n_1} < 0.$$

Then add the numbers  $a^j$  with  $j < n_1$  until

$$a^n - a^{n-1} - a^{n-2} - \dots - a^{n_1} + a^{n_1-1} + \dots + a^{n_2} > 0.$$

Then subtract powers until a sum is  $< 0$  and so on. This algorithm defines the numbers

$$\varepsilon_n, \varepsilon_{n-1}, \dots, \varepsilon_0.$$

The last step consists in adding or subtracting the sum  $1 + a + \dots + a^k$  to or from

$$\varepsilon_{k+1} a^{k+1} + \dots + \varepsilon_n a^n$$

whereby  $|\varepsilon_{k+1} a^{k+1} + \dots + \varepsilon_n a^n| \leq a^{k+1}$  by construction and

$$1 + a + \dots + a^k \leq a^{k+1}.$$

Then

$$\begin{aligned}
 (a-1)|\varepsilon_0 + \varepsilon_0 a + \dots + \varepsilon_n a^n| &= \\
 (a-1)|\varepsilon_{k+1} a^{k+1} + \dots + \varepsilon_n a^n - (1 + a + \dots + a^k)| & \\
 \leq (a-1) \left( a^{k+1} - \sum_{j=0}^k a^j \right) & \\
 = (a-1) \left( a^{k+1} - \frac{a^{k+1} - 1}{a-1} \right) & \\
 = a^{k+1} (a-2) + 1 < 1 &
 \end{aligned}$$

since  $a-2 < 0$ .

Also solved by the proposer.

**Problem 887.** Proposed by D.M. Bătinetu-Giurgiu, “Matei Basarab” National College, Bucharest, Romania and Neculai Stanciu, “George Emil Palade” School, Buzău, Romania.

Prove that in any triangle  $ABC$  with semiperimeter  $s$ , inradius  $r$  and usual notations, the following is true

$$\frac{a^{(m+1)}}{(s-b)^m} + \frac{b^{(m+1)}}{(s-c)^m} + \frac{c^{(m+1)}}{(s-a)^m} \geq 3 * 2^{(m+1)} * \sqrt{3} * r.$$

**Solution** by Ioan Viorel Coddreanu, Satulung, Maramures, Romania.

Using the Radon Inequality, we get

$$\begin{aligned}
 \frac{a^{m+1}}{(s-b)^m} + \frac{b^{m+1}}{(s-c)^m} + \frac{c^{m+1}}{(s-a)^m} &\geq \frac{(a+b+c)^{m+1}}{(s-a+s-b+s-c)^m} \\
 &= \frac{(2s)^{m+1}}{s^m} \\
 &= 2^{m+1} * s.
 \end{aligned}$$

Using the Mitrinovic Inequality,  $s \geq 3\sqrt{3}r$ , we get

$$\frac{a^{m+1}}{(s-b)^m} + \frac{b^{m+1}}{(s-c)^m} + \frac{c^{m+1}}{(s-a)^m} \geq 3 * 2^{m+1} * \sqrt{3} * r.$$

Also solved by Florică Anastase, “Alexandru Odobescu” High School, Lehliu-Gară, Călărași, Romania; Brian Bradie, Christopher Newport University, Newport News, VA; Albert Stadler, Herrliberg, Switzerland; Marian Ursărescu, “Roman-Vodă” National College, Roman, Romania; and the proposer.

**Problem 888.** Proposed by D.M. Bătinetu-Giurgiu, “Matei Basarab” National College, Bucharest, Romania and Neculai Stanciu, “George Emil Palade” School, Buzău, Romania.

Let the positive real sequence  $(a_n)_{n \geq 1}$  be such that  $\lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n \sqrt[n]{(n!)^2}} = a \in \mathbb{R}_+^*$ . Compute

$$\lim_{n \rightarrow \infty} \frac{1}{\sqrt[n]{(2n-1)!!}} \left( \sqrt[n+1]{a_{n+1}} - \sqrt[n]{a_n} \right).$$

**Solution** by Brian Bradie, Christopher Newport University, Newport News, VA.

By Stirling’s approximation,  $n! \sim \sqrt{2\pi n} n^{n+1/2} e^{-n}$ , so

$$\begin{aligned} (2n-1)!! &= \frac{(2n)!}{2^n n!} \sim \frac{(2n)^{2n+\frac{1}{2}} e^{-2n}}{2^n n^{n+\frac{1}{2}} e^{-n}} \\ &= 2^{n+\frac{1}{2}} n^n e^{-n}. \end{aligned}$$

Now, if  $\lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n \sqrt[n]{(n!)^2}} = a$ , then

$$\lim_{n \rightarrow \infty} \frac{a_{n+1}}{n^2 a_n} = \lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n \sqrt[n]{(n!)^2}} * \frac{\sqrt[n]{(n!)^2}}{n^2} = \frac{a}{e^2}.$$

Additionally,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{\sqrt[n]{(2n-1)!!}} \left( \sqrt[n+1]{a_{n+1}} - \sqrt[n]{a_n} \right) \\ &= \lim_{n \rightarrow \infty} \left( \sqrt[n+1]{a_{n+1}} - \sqrt[n]{a_n} \right) * \frac{n}{\sqrt[n]{(2n-1)!!}} \\ &= \frac{e}{2} \lim_{n \rightarrow \infty} \frac{1}{n} \left( \sqrt[n+1]{a_{n+1}} - \sqrt[n]{a_n} \right). \end{aligned}$$

Write

$$\frac{1}{n} \left( \sqrt[n+1]{a_{n+1}} - \sqrt[n]{a_n} \right) = \frac{\sqrt[n]{a_n}}{n^2} * \frac{u_n - 1}{\ln u_n} * \ln u_n^n,$$

where  $u_n = \frac{\sqrt[n+1]{a_{n+1}}}{\sqrt[n]{a_n}}$ . With

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{\sqrt[n]{a_n}}{n^2} &= \lim_{n \rightarrow \infty} \sqrt[n]{\frac{a_n}{n^{2n}}} \\ &= \lim_{n \rightarrow \infty} \frac{a_{n+1}}{(n+1)^{2(n+1)}} * \frac{n^{2n}}{a_n} \\ &= \lim_{n \rightarrow \infty} \frac{a_{n+1}}{n^2 a_n} \left( \frac{n}{n+1} \right)^{2(n+1)} \\ &= \frac{a}{e^2} * \frac{1}{e^2} = \frac{a}{e^4}, \end{aligned}$$

$$\begin{aligned}\lim_{n \rightarrow \infty} u_n &= \lim_{n \rightarrow \infty} \frac{{}^{n+1}\sqrt{a_{n+1}}}{(n+1)^2} * \frac{n^2}{\sqrt[n]{a_n}} \left( \frac{n+1}{n} \right)^2 \\ &= \frac{a}{e^4} * \frac{e^4}{a} * 1 = 1,\end{aligned}$$

$\lim_{n \rightarrow \infty} \frac{u_n - 1}{\ln u_n} = 1$ , and

$$\begin{aligned}\lim_{n \rightarrow \infty} u_n^n &= \lim_{n \rightarrow \infty} \frac{a_{n+1}^{n/(n+1)}}{a_n} \\ &= \lim_{n \rightarrow \infty} \frac{a_{n+1}}{n^2 a_n} * \frac{(n+1)^2}{{}^{n+1}\sqrt{a_{n+1}}} \left( \frac{n}{n+1} \right)^2 \\ &= \frac{a}{e^2} * \frac{e^4}{a} * 1 = e^2,\end{aligned}$$

it follows that

$$\lim_{n \rightarrow \infty} \frac{1}{n} ({}^{n+1}\sqrt{a_{n+1}} - \sqrt[n]{a_n}) = \frac{a}{e^4} * 1 * 2 = \frac{2a}{e^4}.$$

Finally,

$$\lim_{n \rightarrow \infty} \frac{1}{\sqrt[n]{(2n-1)!!}} ({}^{n+1}\sqrt{a_{n+1}} - \sqrt[n]{a_n}) = \frac{e}{2} * \frac{2a}{e^4} = \frac{a}{e^2}.$$

*Also solved by Florică Anastase, “Alexandru Odobescu” High School, Lehliu-Gară, Călărași, Romania; Angel Plaza, Universidad de Las Palmas de Gran Canaria, Spain; Albert Stadler, Herrliberg, Switzerland; Marian Ursărescu, “Roman-Vodă” National College, Roman, Romania; and the proposer.*

**Problem 889.** Proposed by Seán Stewart, Bomaderry, NSW, Australia.

If  $h_n = \sum_{k=1}^{2n} \frac{(-1)^{k+1}}{k}$ , then evaluate the following two limits:

- (i)  $\lim_{n \rightarrow \infty} (\log(2) - h_n) n$ ,
- (ii)  $\lim_{n \rightarrow \infty} (h_n h_{n+1} - \log^2(n)) n$ .

**Solution** by Marian Ursărescu, “Roman-Vodă” National College, Roman, Romania.

(i) We use Cesaro-Stolz for  $\frac{0}{0}$  :

$$\begin{aligned}
 \lim_{n \rightarrow \infty} (\ln 2 - h_n)n &= \lim_{n \rightarrow \infty} \frac{\ln 2 - h_n}{1/n} \\
 &= \lim_{n \rightarrow \infty} \frac{\ln 2 - h_{n+1} - \ln 2 + h_n}{\frac{1}{n+1} - \frac{1}{n}} \\
 &= \lim_{n \rightarrow \infty} \frac{-h_{n+1} + h_n}{-\frac{1}{n(n+1)}} \\
 &= \lim_{n \rightarrow \infty} \frac{\frac{-2n-2+2n+1}{2n(2n+1)}}{-\frac{1}{n(n+1)}} \\
 &= \lim_{n \rightarrow \infty} \frac{n(n+1)}{2n(2n+1)} = \frac{1}{4}.
 \end{aligned}$$

(ii)

$$\begin{aligned}
 \lim_{n \rightarrow \infty} (h_n h_{n+1} - \ln^2(2))n &= \lim_{n \rightarrow \infty} (h_{n+1}h_n - h_n^2 + h_n^2 - \ln^2(2))n \\
 &= \lim_{n \rightarrow \infty} h_n(h_{n+1} - h_n)n + \lim_{n \rightarrow \infty} (h_n^2 - \ln^2(2))n;
 \end{aligned} \tag{1}$$

$$\begin{aligned}
 \lim_{n \rightarrow \infty} h_n(h_{n+1} - h_n)n &= \lim_{n \rightarrow \infty} h_n \left( \frac{1}{2n+1} - \frac{1}{2n+2} \right)n \\
 &= \ln 2 * 0 = 0;
 \end{aligned} \tag{2}$$

$$\begin{aligned}
 \lim_{n \rightarrow \infty} (h_n^2 - \ln^2(2))n &= \lim_{n \rightarrow \infty} (h_n - \ln 2)(h_n + \ln 2)n \\
 &= 2\ln 2 * \left( -\frac{1}{4} \right) \text{ by (i)} \\
 &= -\frac{1}{2}\ln 2.
 \end{aligned} \tag{3}$$

From (1), (2), and (3) it follows that

$$\lim_{n \rightarrow \infty} (h_n h_{n+1} - \ln^2(2))n = -\frac{1}{2}\ln 2.$$

*Also solved by Brian Bradie, Christopher Newport University, Newport News, VA; Steven Jang, Cal Poly Pomona Problem Solving Group, Pomona, CA; Albert Stadler, Herrliberg, Switzerland; and the proposer.*

**Problem 890.** *Proposed by Robert Stanton, St. Johns University, Jamaica, NY.*  
 For digits  $a, b, c, d$ , let  $abcd$  represent the ordinary decimal representation  $10^3a + 10^2b + 10c + d$ . Prove that there is a unique positive integer  $n = aabb$  that is a perfect square.

**Solution** by Steven Jang, Cal Poly Pomona Problem Solving Group, Pomona, CA.

We are going to show that the only possible positive integer is 7744.

1024, 1089, 1156, 1225, 1296, 1369, 1444, 1521, 1600, 1681, 1764, 1849, 1936, 2025, 2116, 2209, 2304, 2401, 2500, 2601, 2704, 2809, 2916, 3025, 3136, 3249, 3364, 3481, 3600, 3721, 3844, 3969, 4096, 4225, 4356, 4489, 4624, 4761, 4900, 5041, 5184, 5329, 5476, 5625, 5776, 5929, 6084, 6241, 6400, 6561, 6724, 6889, 7056, 7225, 7396, 7569, 7744, 7921, 8100, 8281, 8464, 8649, 8836, 9025, 9216, 9409, 9604, 9801.

The only one of the form  $aabb$  is 7744.

*Also solved by Avirup and Biswarup Chakraborty, Narendrapur Ramkrishna Mission Vidyalaya. Class 12; Brian Bradie, Christopher Newport University, Newport News, VA; Brian Beasley, Presbyterian College, Clinton, SC; Henry Ricardo, Westchester Area Math Circle, Purchase, NY; Albert Stadler, Herrliberg, Switzerland; Andrew Volk, Liberty University, Lynchburg, VA; HyunBin Yoo, South Korea; and the proposer.*

**Errata:** In the Fall 2021 issue, Titu Zvonaru was erroneously left off the list of solvers of the following problems: Problems 870, 872, and 873. We seriously apologize for this omission.

## ***Kappa Mu Epsilon News***

Edited by Mark Hughes, Historian  
Updated information as of June 2022

News of chapter activities and other noteworthy KME events should be sent to

Mark Hughes, KME Historian  
Frostburg State University  
Department of Mathematics  
Frostburg, MD 21532  
or to  
mhughes@frostburg.edu

### **KAPPA MU EPSILON**

#### **Chapter News**

##### **AR Beta – Henderson State University**

*Chapter President – Madison Rushing; 68 Total Members; 4 New Members*  
*Other Spring 2022 Officers: Carmen Little, Vice President; Nicole Schranz, Secretary; Rachel Pepper, Treasurer; Fred Worth, Corresponding Secretary; and Carolyn S. Eoff, Faculty Sponsor.*

Due to Covid, our chapter did not have many activities. We did have a picnic in conjunction with our initiation ceremony.

##### **CT Beta – Eastern Connecticut State University**

*Corresponding Secretary and Faculty Sponsor – Dr. Mehdi Khorami; 547 Total Members; 13 New Members*

##### **CT Gamma – Central Connecticut State University**

*Chapter President – William Caron; 78 Total Members*  
*Other Spring 2022 Officers: Bradley Doolgar, Vice President; Emma Johnson, Secretary; Micalyia Douglas, Treasurer; Gurbakhsh Singh, Corresponding Secretary; and Marion Anton, Faculty Sponsor.*

##### **FL Gamma – Southeastern University**

*Chapter President – Elizabeth Davison; 74 Total Members; 7 New Members*  
*Other Spring 2022 Officers: Anna Coleman, Vice President; Jonathan Kurz, Secretary; Jodi Cross, Treasurer; Dr. Berhane Ghaim, Corresponding Secretary and Faculty Sponsor.*

##### **GA Zeta – Georgia Gwinnett College**

*Chapter President – Aviva Kerven; 66 Total Members*

*Other Spring 2022 Officers: Alexa Sheets, Vice President; Hope Doherty, Secretary; William Watts, Treasurer; Dr. Jamye Curry Savage, Corresponding Secretary and Faculty Sponsor; and Dr. Livy Uko, Faculty Sponsor.*

The GA Zeta Chapter had 4 members to attend the Southeastern Regional Convention hosted by the University of North Alabama. Those members were Alexa Sheets, Aviva Kerven, Hope Doherty, and Gabriel Amat. Three of these students presented their research at the convention. The student names and presentation titles were:

- Aviva Kerven – Title: *Algorithms for Topological Invariants of Surfaces*
- Hope Doherty – Title: *The Algebraic Structure of the Determinant of Joined Graphs*
- Gabriel Amat – Title: *Algebraic Structure on the Number of Spanning Trees of Joined Graphs*

The GA Zeta Chapter also had four students to graduate this semester:

- Aviva Kerven – Accepted to the Master's Program in Actuarial Science at Georgia State.
- Alexa Sheets – Applied/Interviewed as a Mathematician to such companies as NSA and Johns Hopkins Applied Physics Laboratory.
- Tyler Smith – Applied/Interviewed for Data Science Jobs such as Atlanta Braves and Sunbelt Baseball League.

### **IA Alpha – University of Northern Iowa**

*Chapter President – Lauren Dierks; 1112 Total Members; 1 New Member*

*Other Spring 2022 Officers: Jacob Metzen, Vice President; Maxwell Tensen, Secretary; Lydia Butters, Treasurer; and Dr. Mark D. Ecker, Corresponding Secretary and Faculty Sponsor.*

Eleven student members of KME and three faculty met face-to-face (for the first time in over two years) on Monday, May 2, 2022 in Wright Hall. Student member Dominic DeKeyser presented his senior seminar project entitled “Madden09 PS2: A Statistical Analysis of Six Simulated Seasons” and one new student member was initiated.

### **IA Delta – Wartburg College**

*Chapter President – David Guetzlaff; 773 Total Members; 5 New Members*

*Other Spring 2022 Officers: Gavin Foust-Wollenberg, Vice President; Samuel Bast, Secretary; Tim Wengenack, Treasurer; Brian Birgen, Corresponding Secretary; and Dr. Chris Allen, Faculty Sponsor.*

Our initiation ceremony was held on April 9, 2022. Audrey Hesse McGarry, a 2009 alum, spoke about Threat Detection.

### **IL Zeta – Dominican University**

*Corresponding Secretary – Mihaela Blanariu; 458 Total Members; 8 New Members*

The Illinois Zeta chapter was excited to initiate eight new members on March 31, 2022 at Dominican University. At the ceremony, Dr. Angela Antonou, Associate Professor of Mathematics at University of St. Francis in Joliet, Illinois, gave a wonderful plenary talk, “A Rectangular Jigsaw Puzzle and its Surprising Mathematical Connections,” about a game of fitting squares into rectangles and how this, amazingly, relates to the Euclidean algorithm and continued fractions. Audience members played with rectangular jigsaw puzzles to get a feel for the game so that they were primed to understand the deeper theory connected to the game—a very fun and engaging way to learn some rich mathematics! Afterwards, participants initiated eight new members of the chapter, many of whom had invited friends and family to share in the celebration.

#### **IN Beta – Butler University**

*Corresponding Secretary – Scott Kaschner; 444 Total Members, 4 New Members  
Other Spring 2022 Officers: Rasitha Jayasekare, Faculty Sponsor.*

New Initiates – Aaron Marshall, Evan Blom, Nicole Dickson, and Jackson Morrill.

#### **KS Beta – Emporia State University**

*Chapter President – Joey Feuerborn; 1539 Total Members; 7 New Members  
Other Spring 2022 Officers: Jeanna Hill, Vice President; Austin Crabtree, Secretary; Katey Dembowski, Treasurer; Tom Mahoney, Corresponding Secretary; and Brian Hollenbeck, Faculty Sponsor.*

The Kansas Beta chapter enjoyed a very social semester. After the February meeting, we had a bowling night. In March, we initiated seven new members at a Pizza Ranch. In April, students hosted an “art night” of acrylic painting. And in May, we gathered for a Color Run.

New Initiates – Julia Whitaker, Joey Feuerborn, Ryan Sauter, Melissa Claypool, Samantha Caron, Tyler O’Dell, and Shane Mattson.

#### **KS Delta – Washburn University**

*Chapter President – Clare Bindley; 834 Total Members; 12 New Members  
Other Spring 2022 Officers: Kael Ecord, Vice President; Ajar Basnet, Secretary; Katherine Cook, Treasurer; and Sarah Cook, Corresponding Secretary and Faculty Sponsor.*

Ten students and two faculty were initiated into the Kansas Delta Chapter of Kappa Mu Epsilon on March 23 through a virtual ceremony. In April, two faculty members (Beth McNamee and Sarah Cook) and five students (Ajar Basnet, Clare Bindley, Ryan Haller, Sanskar Neupane, Gabriel Rose) attended the regional KME North Central Convention in Pittsburg, Kansas. Washburn student Ryan Haller presented his research project on “An Exploration of the Tutte Polynomial”. Ryan was awarded the top prize for his presentation.

New Initiates – Corbin Cool, Lauren Frank, Rajesh Kandel, Jesse Mort, Jr., Sanskar Neupane, Seth Phelps, Graci Renay Postma, Gabriel Rose, Nicolas Schwensen, Calvin Grant Teater, Lori Gill, and Gary Hu.

### MD Alpha – Notre Dame of Maryland University

*Chapter President – Cecia Zavala Ramos; 407 Total Members; 5 New Members*

*Other Spring 2022 Officers: Christina McConnell, Vice President; Erika Kaschak, Secretary; Shawne Ashley Samaco, Treasurer; and Charles Buehrle, Corresponding Secretary and Faculty Sponsor.*

MD Alpha items are below.

New Initiates – Isabella Dallasta, Shawne Samaco, Janelle Sanglang, Bintou Timbine, and Brigitte Flores.



### MD Delta – Frostburg State University

*Chapter President – Ashley Armbruster; 543 Total Members; 3 New Members*

*Other Spring 2022 Officers: Brynn Lewis, Vice President; Jessica Farrell, Secretary; Jay Collins, Treasurer; Mark Hughes, Corresponding Secretary and Faculty Sponsor; and Frank Barnet, Faculty Sponsor.*

Maryland Delta Chapter had meetings in February, March, and April where we enjoyed pizza, math videos and puzzles. We had a successful Pi-Day bake sale on March 14. It was nice to be able to resume this annual activity after having missed it last year due to Covid. In early April, we were pleased to welcome three new members. At the Initiation Ceremony, faculty sponsor Dr. Mark Hughes presented a lecture entitled “Two Theorems on Polyhedra”. We finished our semester with a picnic in May where we had a lot of fun and enjoyed some great weather. New Initiates – Kaitlyn Henderson-Adams, Faith James Sargent, and Adam Sullivan.

### MI Beta – Central Michigan University

*Chapter President – Kelsey Knoblock; 1761 Total Members; 3 New Members*

*Other Spring 2022 Officers: Emily Naegelin, Vice President; Jenna Wazny, Secretary; Jeremy Proksch, Treasurer; and Dr. Dmitry Zakharov, Corresponding Secretary and Faculty Sponsor.*

In the Spring semester, the Michigan Beta Chapter held 6 general meetings, a book sale fundraiser, and an end-of-semester volunteer tutoring event. The meetings included two research talks by CMU professors, Dr. Jordan Watts and Dr.

Dmitry Zakharov. The chapter also hosted a math bingo night, a scavenger hunt, and a Pictionary game.

### **MO Beta – University of Central Missouri**

*Chapter President – Haleigh Clark; 1549 Total Members, 8 New Members (5 from Fall 2021)*

*Other Spring 2022 Officers: Paige Van Blarcum, Vice President and Treasurer; Connor Stohr, Secretary; Brianna Ward, Historian; Blaise Heider, Faculty Sponsor; Paul Plummer, Faculty Sponsor; and Steven Shattuck, Corresponding Secretary and Faculty Sponsor.*

The Missouri Beta Chapter of Kappa Mu Epsilon had monthly meetings for Fall 2021 and Spring 2022. Programming at these meetings include: a talk on LaTeX, reports from students about their summer internships/REU experiences, math jeopardy and other math games. The Missouri Beta chapter attended both the South Central and North Central regional meetings.

New Initiates – Spring 2022: Andrew Barnes, Lindsey Edmonds, Jada Oldham; Fall 2021: Karissa Abrolat, Luke George, John Mason Hocking, Hannah Noel, and Hilari Waters

### **MO Kappa – Drury University**

*Chapter President – Aspen Hill; 330 Total Members; 19 New Members*

*Other Spring 2022 Officers: Charlie Roder, Vice President; Levi Graham, Secretary and Corresponding Secretary; Dani Brown, Treasurer; and Collin T. Baker, Faculty Sponsor.*

New Initiates – Sam Black, Dani Brown, Matthew Dalton, Julian Fisher, Kelsi Gelle, Levi Graham, Aspen Hill, Lindsey Kollmeyer, Brandon Lacy, Micah Lehenbauer, Sean Lowry, Marina Martins Amorim, Laura Pareja Prieto, John Rice, Charlie Roder, Bryan Valencia, Ean Vandergraaf, Brooke Weider, and Carter Williams.

### **MO Theta – Evangel University**

*Chapter President – Peter Russell; 298 Total Members; 4 New Members*

*Other Spring 2022 Officers: Jack Lin, Vice President; and Dianne Twigger, Corresponding Secretary and Faculty Sponsor.*

This spring we held three meetings including our annual initiation. We elected a new vice president, Jack Lin, as Hannah Tower graduated this spring. Six students and two faculty attended the North Central Regional convention at Pittsburg State University. We had one presenter (Peter Russell).

New Initiates – Jack Lin, Hayden Pyle, Victoria Risner, and Peyton Twigg.

### **NC Zeta – Catawba College**

*Chapter President – Maria Arnold; 103 Total Members; 4 New Members*

*Other Spring 2022 Officers: Abigail Hartman, Vice President; Ofek Malul, Secretary; Jackson Chapin, Treasurer; and Dr. Katherine Baker, Corresponding Secretary and Faculty Sponsor.*

**NE Gamma – Chadron State College**

*Chapter President – Dylan Koretko; 544 Total Members*

*Other Spring 2022 Officers: Kyeisha Garza, Vice President; Manou Mbombo, Secretary; Louis Christopher, Treasurer; and Gregory Moses, Corresponding Secretary and Faculty Sponsor.*

**NJ Epsilon – New Jersey City University**

*Corresponding Secretary and Faculty Sponsor – Dr. Alemtsehai Turasie; 151 Total Members*

*Other Spring 2022 Officer: Dr. Debananda Chakraborty, Faculty Sponsor.*

**NY Lambda – LIU Post**

*Chapter President – Timothy Nagorsky; 470 Total Members; 7 New Members*

*Other Spring 2022 Officer: Dr. Corbett Redden, Corresponding Secretary and Faculty Sponsor.*

**NY Nu – Hartwick College**

*Chapter President – Dell Potts; 349 Total Members*

*Other Spring 2022 Officers: Shane Lamparter, Vice President; Hannah Bochniak, Secretary; James Lukasik, Treasurer; and Min Chung, Corresponding Secretary and Faculty Sponsor.*

**OH Gamma – Baldwin Wallace University**

*Chapter President – Harrison Rouse; 1041 Total Members; 14 New Members*

*Other Spring 2022 Officers: Izzy Andrews, Vice President; Moore Syrowski, Secretary; and David Calvis, Corresponding Secretary and Faculty Sponsor.*

Annual initiation ceremony held March 27, 2022 in our lovely new Knowlton Center.

New Initiates – Grace Fryling, Julia Gersey, Julia Grady, David Hudson, Hannah Ogden, Brian Parnitzke, Zachary Pietrasz, Dana Rabung, Ryan Reffner, Hannah Ross, Chloe Sperry, Parker Stevens, Emma Trost, and Ashley Workman.

**OK Delta – Oral Roberts University**

*Chapter President – Gladys Chen; 214 Total Members; 7 New Members*

*Other Spring 2022 Officers: Abigail E. Lea, Vice President; Anna K. Kinnunen, Secretary; Nathaniel P. Youmans, Treasurer; and Dr. Enrique Valderrama Araya, Corresponding Secretary and Faculty Sponsor.*

New Initiates – Gladys Chen, Anna K. Kinnunen, Abigail E. Lea, Shaofan Li, Aidan Samuel Wright, Andrew B. Westlund, and Nathaniel P. Youmans.

**PA Mu – Saint Francis University**

*Chapter President – Michael Gallagher; 510 Total Members; 16 New Members*

*Other Spring 2022 Officers: Morgan Kiesewetter, Vice President; Regina Edgington, Secretary; Jared Ohler, Treasurer; and Dr. Brendon LaBuz, Corresponding*

*Secretary and Faculty Sponsor.*

The Pennsylvania Mu Chapter was pleased to serve free pie to the campus community again for Pi Day on March 14<sup>th</sup>. Fifteen students and one faculty member were initiated into the Pennsylvania Mu Chapter on Monday April 4<sup>th</sup>. The ceremony was held at 5:00 p.m. in the atrium of the Science Center. Faculty initiate Brother Marius Strom gave an opening prayer before dinner. After dinner KME faculty member Dr. Ying Li presented *The Fibonacci Sequence* where she told us about some interesting and unusual facts about the famous Fibonacci sequence. The initiation ceremony followed and we celebrated our 500<sup>th</sup> member.

**PA Pi – Slippery Rock University**

*Chapter President – Spencer Kahley; 145 Total Members; 5 New Members*

*Other Spring 2022 Officers: Boris Brimkov, Corresponding Secretary; and Amanda Goodrick, Faculty Sponsor.*

We held an initiation ceremony attended by department faculty and new KME members. The initiates each gave a presentation on their research.

**PA Rho – Thiel College**

*Chapter President – Ethan Stishan; 145 Total Members; 6 New Members*

*Other Spring 2022 Officers: Camryn Sankey, Vice President; Cassie Brown, Secretary; Kara Baumgardner, Treasurer; Dr. Russell Richins, Corresponding Secretary; and Dr. Jie Wu, Faculty Sponsor.*

We had our initiation ceremony in April and several meetings throughout the semester.

**RI Beta – Bryant University**

*Corresponding Secretary – Prof. John Quinn; 200 Total Members; 12 New Members*

*Other Spring 2022 Officer: Prof. Gao Niu, Faculty Sponsor.*

We held our annual Math Honors ceremony at Bryant University on Thursday, April 28, 2022. We initiated 12 new student members into the RI Beta Chapter of KME. We have do not have a student executive board for this upcoming academic year, as of yet.

**TN Gamma – Union University**

*Chapter President – Braden Watkins; 524 Total Members; 7 New Members*

*Other Spring 2022 Officers: Joya Schrock, Vice President; Rylee Iorio, Secretary; Taylor Overcast, Treasurer; Bryan Dawson, Corresponding Secretary; and Matt Lunsford, Faculty Sponsor.*

Chapter officers repainted the “Union Intersection” walls with chalkboard paint; the results have been an abundance of mathematics, humor, and artistry. Our annual initiation banquet was held at Brooksie’s Barn. Two faculty members and three students attended the Southeast region conference in Florence, Alabama. Two of our students, Lisa Reed and Braden Watkins, presented their work at the

conference.

New Initiates – Ian Banderchuk, Paige Bogard, Samantha Burket, Jacob Carbonell, Elizabeth Joy Lewis, Conitra Morgan, and Jessica Searl.

**TX Lambda – Trinity University**

*Corresponding Secretary and Faculty Sponsor – Dr. Hoa Nguyen; 315 Total Members; 8 New Members*

**WV Alpha – Bethany College**

*Chapter President – Amanda M. Reynolds; 198 Total Members; 4 New Members  
Other Spring 2022 Officers: Jacob C. Thornburg, Vice President; Lauren E. Starr, Secretary and Treasurer; and Dr. Adam C. Fletcher, Corresponding Secretary and Faculty Sponsor.*

West Virginia Alpha, like many other chapters across the country, continued to adjust to life in a pandemic. The College returned to life on-campus this year, with strict COVID protocols in place throughout. The local and national restrictions canceled or postponed a number of the chapter's usual activities, like mathematics competitions and professional gatherings. West Virginia Alpha chapter and our local Mathematics and Computer Science Club continued to attend meetings virtually and host small chess and gaming tournaments on campus. The West Virginia Alpha chapter welcomed four new members into its ranks in the spring in-person ceremony and assisted in the initiation of two members in the Upsilon Pi Epsilon computing sciences honor society at its corresponding ceremony.

New Initiates – Geoffrey P. Foster, Ian A. Nelson, Grace A. Omecinski, and Michael D. Ross.

# Active Chapters of Kappa Mu Epsilon

*Listed by date of installation*

Chapter	Location	Installation Date
OK Alpha	Northeastern State University, Tahlequah	18 Apr 1931
IA Alpha	University of Northern Iowa, Cedar Falls	27 May 1931
KS Alpha	Pittsburg State University, Pittsburg	30 Jan 1932
MO Alpha	Missouri State University, Springfield	20 May 1932
MS Alpha	Mississippi University for Women, Columbus	30 May 1932
NE Alpha	Wayne State College, Wayne	17 Jan 1933
KS Beta	Emporia State University, Emporia	12 May 1934
AL Alpha	Athens State University, Athens	5 Mar 1935
NM Alpha	University of New Mexico, Albuquerque	28 Mar 1935
IL Beta	Eastern Illinois University, Charleston	11 Apr 1935
AL Beta	University of North Alabama, Florence	20 May 1935
AL Gamma	University of Montevallo, Montevallo	24 Apr 1937
OH Alpha	Bowling Green State University, Bowling Green	24 Apr 1937
MI Alpha	Albion College, Albion	29 May 1937
MO Beta	University of Central Missouri, Warrensburg	10 Jun 1938
TX Alpha	Texas Tech University, Lubbock	10 May 1940
KS Gamma	Benedictine College, Atchison	26 May 1940
IA Beta	Drake University, Des Moines	27 May 1940
TN Alpha	Tennessee Technological University, Cookeville	5 Jun 1941
MI Beta	Central Michigan University, Mount Pleasant	25 Apr 1942
NJ Beta	Montclair State University, Upper Montclair	21 Apr 1944
IL Delta	University of St. Francis, Joliet	21 May 1945
KS Delta	Washburn University, Topeka	29 Mar 1947
MO Gamma	William Jewell College, Liberty	7 May 1947
TX Gamma	Texas Woman's University, Denton	7 May 1947
WI Alpha	Mount Mary College, Milwaukee	11 May 1947
OH Gamma	Baldwin-Wallace College, Berea	6 Jun 1947
MO Epsilon	Central Methodist College, Fayette	18 May 1949
MS Gamma	University of Southern Mississippi, Hattiesburg	21 May 1949
IN Alpha	Manchester College, North Manchester	16 May 1950
PA Alpha	Westminster College, New Wilmington	17 May 1950
IN Beta	Butler University, Indianapolis	16 May 1952
KS Epsilon	Fort Hays State University, Hays	6 Dec 1952
PA Beta	LaSalle University, Philadelphia	19 May 1953
VA Alpha	Virginia State University, Petersburg	29 Jan 1955
IN Gamma	Anderson University, Anderson	5 Apr 1957
CA Gamma	California Polytechnic State University, San Luis Obispo	23 May 1958
TN Beta	East Tennessee State University, Johnson City	22 May 1959
PA Gamma	Waynesburg College, Waynesburg	23 May 1959
VA Beta	Radford University, Radford	12 Nov 1959
NE Beta	University of Nebraska—Kearney, Kearney	11 Dec 1959
IN Delta	University of Evansville, Evansville	27 May 1960
OH Epsilon	Marietta College, Marietta	29 Oct 1960
MO Zeta	University of Missouri—Rolla, Rolla	19 May 1961
NE Gamma	Chadron State College, Chadron	19 May 1962
MD Alpha	College of Notre Dame of Maryland, Baltimore	22 May 1963
CA Delta	California State Polytechnic University, Pomona	5 Nov 1964
PA Delta	Marywood University, Scranton	8 Nov 1964
PA Epsilon	Kutztown University of Pennsylvania, Kutztown	3 Apr 1965
AL Epsilon	Huntingdon College, Montgomery	15 Apr 1965
PA Zeta	Indiana University of Pennsylvania, Indiana	6 May 1965
TN Gamma	Union University, Jackson	24 May 1965
IA Gamma	Morningside College, Sioux City	25 May 1965
MD Beta	McDaniel College, Westminster	30 May 1965
IL Zeta	Dominican University, River Forest	26 Feb 1967
SC Beta	South Carolina State College, Orangeburg	6 May 1967
PA Eta	Grove City College, Grove City	13 May 1967
NY Eta	Niagara University, Niagara University	18 May 1968
MA Alpha	Assumption College, Worcester	19 Nov 1968
MO Eta	Truman State University, Kirksville	7 Dec 1968
IL Eta	Western Illinois University, Macomb	9 May 1969
OH Zeta	Muskingum College, New Concord	17 May 1969
PA Theta	Susquehanna University, Selinsgrove	26 May 1969
PA Iota	Shippensburg University of Pennsylvania, Shippensburg	1 Nov 1969
MS Delta	William Carey College, Hattiesburg	17 Dec 1970
MO Theta	Evangel University, Springfield	12 Jan 1971
PA Kappa	Holy Family College, Philadelphia	23 Jan 1971
CO Beta	Colorado School of Mines, Golden	4 Mar 1971
KY Alpha	Eastern Kentucky University, Richmond	27 Mar 1971
TN Delta	Carson-Newman College, Jefferson City	15 May 1971
NY Iota	Wagner College, Staten Island	19 May 1971
SC Gamma	Winthrop University, Rock Hill	3 Nov 1972
IA Delta	Wartburg College, Waverly	6 Apr 1973
PA Lambda	Bloomsburg University of Pennsylvania, Bloomsburg	17 Oct 1973
OK Gamma	Southwestern Oklahoma State University, Weatherford	1 May 1973

NY Kappa	Pace University, New York	24 Apr 1974
TX Eta	Hardin-Simmons University, Abilene	3 May 1975
MO Iota	Missouri Southern State University, Joplin	8 May 1975
GA Alpha	State University of West Georgia, Carrollton	21 May 1975
WV Alpha	Bethany College, Bethany	21 May 1975
FL Beta	Florida Southern College, Lakeland	31 Oct 1976
WI Gamma	University of Wisconsin—Eau Claire, Eau Claire	4 Feb 1978
MD Delta	Frostburg State University, Frostburg	17 Sep 1978
IL Theta	Benedictine University, Lisle	18 May 1979
PA Mu	St. Francis University, Loretto	14 Sep 1979
AL Zeta	Birmingham-Southern College, Birmingham	18 Feb 1981
CT Beta	Eastern Connecticut State University, Willimantic	2 May 1981
NY Lambda	C.W. Post Campus of Long Island University, Brookville	2 May 1983
MO Kappa	Drury University, Springfield	30 Nov 1984
CO Gamma	Fort Lewis College, Durango	29 Mar 1985
NE Delta	Nebraska Wesleyan University, Lincoln	18 Apr 1986
TX Iota	McMurry University, Abilene	25 Apr 1987
PA Nu	Ursinus College, Collegeville	28 Apr 1987
VA Gamma	Liberty University, Lynchburg	30 Apr 1987
NY Mu	St. Thomas Aquinas College, Sparkill	14 May 1987
OH Eta	Ohio Northern University, Ada	15 Dec 1987
OK Delta	Oral Roberts University, Tulsa	10 Apr 1990
CO Delta	Mesa State College, Grand Junction	27 Apr 1990
PA Xi	Cedar Crest College, Allentown	30 Oct 1990
MO Lambda	Missouri Western State College, St. Joseph	10 Feb 1991
TX Kappa	University of Mary Hardin-Baylor, Belton	21 Feb 1991
SC Delta	Erskine College, Due West	28 Apr 1991
NY Nu	Hartwick College, Oneonta	14 May 1992
NH Alpha	Keene State College, Keene	16 Feb 1993
LA Gamma	Northwestern State University, Natchitoches	24 Mar 1993
KY Beta	Cumberland College, Williamsburg	3 May 1993
MS Epsilon	Delta State University, Cleveland	19 Nov 1994
PA Omicron	University of Pittsburgh at Johnstown, Johnstown	10 Apr 1997
MI Delta	Hillsdale College, Hillsdale	30 Apr 1997
MI Epsilon	Kettering University, Flint	28 Mar 1998
MO Mu	Harris-Stowe College, St. Louis	25 Apr 1998
GA Beta	Georgia College and State University, Milledgeville	25 Apr 1998
AL Eta	University of West Alabama, Livingston	4 May 1998
PA Pi	Slippery Rock University, Slippery Rock	19 Apr 1999
TX Lambda	Trinity University, San Antonio	22 Nov 1999
GA Gamma	Piedmont College, Demorest	7 Apr 2000
LA Delta	University of Louisiana, Monroe	11 Feb 2001
GA Delta	Berry College, Mount Berry	21 Apr 2001
TX Mu	Schreiner University, Kerrville	28 Apr 2001
CA Epsilon	California Baptist University, Riverside	21 Apr 2003
PA Rho	Thiel College, Greenville	13 Feb 2004
VA Delta	Marymount University, Arlington	26 Mar 2004
NY Omicron	St. Joseph's College, Patchogue	1 May 2004
IL Iota	Lewis University, Romeoville	26 Feb 2005
WV Beta	Wheeling Jesuit University, Wheeling	11 Mar 2005
SC Epsilon	Francis Marion University, Florence	18 Mar 2005
PA Sigma	Lycoming College, Williamsport	1 Apr 2005
MO Nu	Columbia College, Columbia	29 Apr 2005
MD Epsilon	Stevenson University, Stevenson	3 Dec 2005
NJ Delta	Centenary College, Hackettstown	1 Dec 2006
NY Pi	Mount Saint Mary College, Newburgh	20 Mar 2007
OK Epsilon	Oklahoma Christian University, Oklahoma City	20 Apr 2007
HA Alpha	Hawaii Pacific University, Waipahu	22 Oct 2007
NC Epsilon	North Carolina Wesleyan College, Rocky Mount	24 Mar 2008
NY Rho	Molloy College, Rockville Center	21 Apr 2009
NC Zeta	Catawba College, Salisbury	17 Sep 2009
RI Alpha	Roger Williams University, Bristol	13 Nov 2009
NJ Epsilon	New Jersey City University, Jersey City	22 Feb 2010
NC Eta	Johnson C. Smith University, Charlotte	18 Mar 2010
AL Theta	Jacksonville State University, Jacksonville	29 Mar 2010
GA Epsilon	Wesleyan College, Macon	30 Mar 2010
FL Gamma	Southeastern University, Lakeland	31 Mar 2010
MA Beta	Stonehill College, Easton	8 Apr 2011
AR Beta	Henderson State University, Arkadelphia	10 Oct 2011
PA Tau	DeSales University, Center Valley	29 Apr 2012
TN Zeta	Lee University, Cleveland	5 Nov 2012
RI Beta	Bryant University, Smithfield	3 Apr 2013
SD Beta	Black Hills State University, Spearfish	20 Sept 2013
FL Delta	Embry-Riddle Aeronautical University, Daytona Beach	22 Apr 2014
IA Epsilon	Central College, Pella	30 Apr 2014
CA Eta	Fresno Pacific University, Fresno	24 Mar 2015
OH Theta	Capital University, Bexley	24 Apr 2015
GA Zeta	Georgia Gwinnett College, Lawrenceville	28 Apr 2015
MO Xi	William Woods University, Fulton	17 Feb 2016
IL Kappa	Aurora University, Aurora	3 May 2016
GA Eta	Atlanta Metropolitan University, Atlanta	1 Jan 2017
CT Gamma	Central Connecticut University, New Britain	24 Mar 2017
KS Eta	Sterling College, Sterling	30 Nov 2017
NY Sigma	College of Mount Saint Vincent, The Bronx	4 Apr 2018
PA Upsilon	Seton Hill University, Greensburg	5 May 2018

KY Gamma  
MO Omicron  
AK Gamma  
GA Theta

Bellarmino University, Louisville  
Rockhurst University, Kansas City  
Harding University, Searcy  
College of Coastal Georgia, Brunswick

23 Apr 2019  
13 Nov 2020  
27 Apr 2021  
22 Oct 2021