THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF MATHEMATICS

ELLIPTIC CURVES AND THEIR INTEGRATION INTO AN EXISTING UNDERGRADUATE NUMBER THEORY COURSE

LAUREN JEANETTE MINNER
SPRING 2018

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Mathematics
with honors in Mathematics

Reviewed and approved* by the following:

Paul Becker
Associate Professor of Mathematics
Thesis Supervisor

Daniel Galiffa
Associate Professor of Mathematics
Honors Adviser

*Signatures are on file in the Schreyer Honors College.

Abstract

In this thesis, we propose integrating the basic concepts of finite fields and elliptic curves into an undergraduate number theory course and discuss the basic concepts that could be built upon existing course material. The purpose of this is to introduce and prepare students for the possible study of this material in graduate school. We also aim to identify a few crypographical algorithms commonly used in online communication, and explain how such algorithms work when integrated with elliptic curves.

Table of Contents

List of Tables

List of Figures

Acknowledgements

First, I would like to acknowledge Dr. Paul Becker for all his assistance and patience during the creation of this thesis. Without his help, both as my thesis advisor and formerly as my professor for both Introduction to Number Theory and Abstract Algebra, I would not have been able to get through writing the first chapter.

I would also like to thank my honors advisor, Dr. Daniel Joseph Galiffa. Without having taken his Math 141 course as a freshman, I am not sure I would have considered majoring in mathematics until much later in my academic career. I also appreciate all of the help, guidance, and support he has shown me as my professor, research professor, and academic advisor throughout these past three years.

Also, thank you to my friends and family who supported me and put up with my absences and late nights as I was completing this. Even though most of them would never actually want to read this, due to their lack of backgrounds in math, they still regularly supported me.

Lastly, thank you to my dog, Jayne, who despite not understanding any part of what I have been working on, still was happy to curl up with me on the couch or at my desk while I wrote this. That he never tried to eat my computer was also very much appreciated.

Introduction

With the rapid advancement of technology, finding and implementing secure systems of communication has become vital to our daily lives. From online shopping to checking our bank accounts to submitting tax forms, we place our trust in these crypotological algorithms to keep our personal and financial information private from prying eyes. This increasing need for security has helped propel the study of cryptography, which in turn has pushed the need for study in Number Theory, specifically with regards to prime numbers and primality tests. Given the processing capability of our modern computers, determining large prime numbers via a "brute force" method has become easier, making it easier for would-be hackers to break through an algorithm that relies on relatively small primes. Because of this, determining prime numbers with massive numbers of digits (currently, the largest known prime number has 23,249,425 digits) is necessary for our current cryptographical systems to maintain the expectedly high levels of security. In tandem with determining new primes, finding new algorithms to secure information online has also become paramount.

In this paper, we will discuss one of the concepts behind a few of those new algorithms, elliptic curves. Elliptic curves have seen recent importance due to their use in the proof of Fermat's Last Theorem as well as in cryptography. Given this, it is puzzling that most students will not see or hear much about elliptic curves in the classroom until they enter graduate school. Because of this, we discuss some of rudimentary concepts necessary to begin to understand elliptic curves at an undergraduate level, and propose how these concepts might be added to an existing undergraduate mathematics course, Introduction to Number Theory. To aid in understanding why these concepts are important and practical, we also briefly discuss the use of elliptic curves in cryptography, specifically outlining the basic steps of the Elliptic Curve Diffie-Hellman analogue, which is a public-key algorithm already implemented by online entities such as Bitcoin.

Understandably, implementing this additional material may not be practical for every professor overseeing the course on Number Theory, nor for every group of students enrolled. This is not intended to replace any existing course material on cryptography, but rather to add to that material. With this in mind, it is important to begin by covering which preexisting course materials are necessary for the understanding of elliptic curves and elliptic curve cryptography.

Chapter 1

Undergraduate Curriculum

Before discussing the addition of the concept of elliptic curves into a course on number theory and their ties to cryptography, we first must determine what concepts already exist within the course are necessary for understanding how to use elliptic curves. As noted in the introduction, since different professors may approach the course with different curriculum and goals, and different student groups may get through the material at different rates, it is necessary to note that it may not always be possible or practical for finite fields and elliptic curves to appear in a number theory course during a given semester. For this reason, it is important to outline what specific topics must first be covered, and roughly when the concepts discussed in this paper can be introduced into a class in order for proper coverage of the material and optimal student comprehension.

By questioning the various professor at Penn State Behrend who have taught the Math 465: Number Theory course, I have been able to construct a rough list of the topics that should be covered in the first half of the semester.

First, the Division Algorithm, which is explained in further detail on page 5 in Chapter 2 of this paper, typically denoted as

$$a(x) = q(x)b(x) + r(x), \text{ where } |r(x)| < b(x),$$

is one of the first concepts that is necessary for understanding fields and elliptic curves. Fortunately, since it is a basis for most other concepts in a number theory course, this algorithm is almost unanimously taught in the very beginning of the course by each of the professors questioned.

Second, prime numbers, prime factorization, and primality testing should be covered, given that prime numbers and their properties are essential in modular arithmetic, group theory, rings, fields, cryptography and, of course, elliptic curves.

Next, modular arithmetic and equivalence classes need to be introduced and understood, followed by, in no particular order: an introduction to Group Theory, Primitive Roots, Fermat's Little Theorem, and preferably, polynomial factorization using modular arithmetic. Polynomial factorization is not a prerequisite for this paper, given that the division algorithm is being used, but it is helpful in understanding better how fields and, specifically, finite fields are generated and used. Also, as a note, Fermat's Little Theorem can be denoted using either of these two congruences:

$$a^n \equiv a \pmod{n}, \text{ or}$$

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

where $a, n \in \mathbb{Z}$ and n is prime.

Finally, rings and fields should be introduced by mid-semester. This will allow the class to quickly cover the basic theory behind these two topics before moving into the study of finite fields, elliptic curves, and finally, elliptic curve cryptography.

Chapter 2

Finite Fields

2.1 Preliminary Information

In order to understand elliptic curves, students first need to understand the concept of fields. Now, elliptic curves can have points on any field, such as $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$. However, the set of solutions for an elliptic curve equation over a finite field is a finite group, which is essential for its applications to cryptography. So in this chapter, we cover the basics of finite fields.

Let us start by defining a *field* $\mathbb{F}$ as $\mathbb{F} = (S \neq \emptyset, +, \cdot)$, such that $0 \in S, 1 \in S$, that satisfies the following axioms:

1. The two binary operations are commutative:
$$\forall x, y, \quad x + y = y + x, \quad \text{and} \quad x \cdot y = y \cdot x$$
2. The two binary operations are associative:
$$\forall x, y, z, \quad (x + y) + z = x + (y + z), \quad \text{and} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$
3. The identity elements 0 and 1 exist in the field, $\mathbb{F}$:
$$\forall x, \quad x + 0 = x, \quad \text{an} \quad x \cdot 1 = x$$
4. The inverse elements exist in $\mathbb{F}$, $\forall x \in S, \exists! \, (-x) \in S, \ (x^{-1}) \in S$:
$$x - x = 0, \quad \text{and} \quad x \cdot \left(x^{-1}\right) = 1, \ \ x \neq 0$$
5. The distributive property holds:
$$\forall x, y, z, \quad x \cdot (y + z) = x \cdot y + x \cdot z$$

Given that it is a prerequisite for Penn State for students to have taken a mathematical proofs course prior to a course in number theory and that it has already been recommended in this paper that rings and fields be introduced to the class before delving into finite fields and eventually elliptic curve cryptography, these axioms should already be familiar to students.

First, we need the following lemma:

Lemma 2.1.1 *If $\mathbb{F}$ is a field, then the set of polynomials $\mathbb{F}[x]$ with coefficients in $\mathbb{F}$ forms a ring with identity.*

As noted in Chapter 1, the Division Algorithm is the backbone for many concepts in Number Theory, with finite fields and elliptic curves as no exception. For referencing purposes, the Division Algorithm is stated below:

Theorem 2.1.2 *Let $a(x), b(x) \in \mathbb{F}[x], b(x) \neq 0$; then $\exists!$ polynomials q(x) and r(x) with $deg(r(x)) < deg(b(x))$, such that*
$$a(x) = q(x)b(x) + r(x).$$

This algorithm initially becomes necessary when explaining the concept of ideals in a field. Recall from the basics on ring and field theory that an ideal, I, of a field, $\mathbb{F}$, satisfies $nI \subset I$ and $In \subset I$, $\forall n \in \mathbb{F}$. From this, we go on to define a maximal ideal, which is an ideal that is only a subset of the field itself and not of any other ideal of said field.

From [Jud], we obtain the following theorem regarding maximal ideals in rings:

Theorem 2.1.3 *Let $\mathbb{F}$ be a field and suppose that $p(x) \in \mathbb{F}[x]$. Then the ideal generated by p(x) is maximal if and only if p(x) is irreducible.*

PROOF: Given that this theorem possess an "if and only if" statement, we must break the proof into two cases.

CASE 1: Suppose that the polynomial $p(x)$ generates the maximal ideal $\langle p(x)\rangle$ of $\mathbb{F}[x]$. Then $\langle p(x)\rangle$ is also a prime ideal of $\mathbb{F}[x]$. Since a maximal ideal must be properly contained in $\mathbb{F}[x]$, $p(x)$ cannot be a constant polynomial, or a polynomial whose output is always some constant value c.

Let us then assume, by way of contradiction, that $p(x)$ can be factored into two polynomials of lesser degree, such that $p(x) = f(x)g(x)$. Since $\langle p(x)\rangle$ is a prime ideal, one of these factors, which without loss of generality, say $f(x)$, is in $\langle p(x)\rangle$ and thus is a multiple of $p(x)$. However, as we defined on the previous page, if $f(x)$ is an ideal in $\langle p(x)\rangle$, then $f(x) = h(x)f(x) \in \langle p(x)\rangle$ for some polynomial $h(x)$, and $h(x)f(x) \subset \langle f(x)\rangle$. This implies that $\langle p(x)\rangle \subset < f(x) >$, which contradicts our earlier assumption that $\langle p(x)\rangle$ is maximal. Therefore, $p(x)$ is irreducible over $\mathbb{F}[x]$ when the ideal generated by $p(x)$ is maximal.

CASE 2: Suppose that $p(x)$ is irreducible over $\mathbb{F}[x]$.

Let H be an ideal in $\mathbb{F}[x]$ containing $\langle p(x)\rangle$, where $H = \langle f(x)\rangle$ for some $f(x) \in \mathbb{F}[x]$. Since $p(x) \in H$, it must be true that $p(x) = f(x)g(x)$ for some $g(x) \in \mathbb{F}[x]$. However, we already established that $p(x)$ is irreducible, so either $f(x)$ or $g(x)$ must be a constant polynomial. If $f(x)$ is a constant polynomial, then $H = \mathbb{F}[x]$, indicating that the ideal containing and generated by $p(x)$ is maximal (since it is the field itself). If instead $g(x)$ is constant, then $f(x)$ is a constant multiple of $\langle p(x)\rangle$ and $H = \langle p(x)\rangle$. Therefore, $\langle p(x)\rangle$ is not a subset of another proper ideal of $\mathbb{F}[x]$, and is a maximal ideal.

The usefulness of this maximal ideal can be shown to students using an example common in various texts, which has been provided below.

2.1.1 Example from [Jud]

Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Since neither 0 nor 1 is a root of this polynomial, we know that $p(x)$ is irreducible over $\mathbb{Z}_2$. We will construct a field extension of $\mathbb{Z}_2$ containing an element α such that $p(\alpha) = 0$. By **Theorem 2.1.3**, the ideal $\langle p(x)\rangle$ generated by $p(x)$ is maximal; hence, $\mathbb{Z}_2[x]/\langle p(x)\rangle$ is a field. Let $f(x) + \langle p(x)\rangle$ be an arbitrary element of $\mathbb{Z}_2[x]/\langle p(x)\rangle$. By the division algorithm (**Theorem 2.1.2**),

$$f(x) = (x^2 + x + 1)q(x) + r(x),$$

where the degree of $r(x)$ is less than the degree of $x^2 + x + 1$. This means that the only possible values for r(x) are 0, 1, x, and $x+1$. Thus, if we let $\mathbb{E} = Z_2[x]/\langle x^2 + x + 1\rangle$, $\mathbb{E}$ is a field containing four elements and must be a field extension of $\mathbb{Z}_2$ containing a zero of $p(x)$, which we'll denote as

a. This field consists of the elements

$$0 + 0a = 0$$
$$1 + 0a = 1$$
$$0 + 1a = a$$
$$1 + 1a = 1 + a$$

From **Theorem 2.1.2**, $a^2 + a + 1 = (a^2 + a + 1)(1) + 0$, so $a^2 = 1 + a$, and computing $(1 + a)^2$, we get $1 + 2a + a^2 = 1 + (1 + a) = a$. Using these and similar calculations, we can construct the following addition and multiplication tables.

+	0	1	a	$1 + a$
0	0	1	a	$1 + a$
1	1	0	$1 + a$	a
a	a	$1 + a$	0	1
$1 + a$	$1 + a$	a	1	0

Table 2.1: Addition Table for $\mathbb{E}$

$*$	0	1	a	$1 + a$
0	0	0	0	0
1	0	1	a	$1 + a$
a	0	a	$1 + a$	1
$1 + a$	0	$1 + a$	1	a

Table 2.2: Multiplication Table for $\mathbb{E}$

2.2 Finite Fields

From the name, *finite fields*, also denoted as *Galois fields* after the mathematician, Évariste Galois, are fields containing a finite number of elements that still satisfy the previously defined field axioms. So, a finite field containing q elements, where $q = p^k$ for some prime p and positive integer k, exists with order q, where the *order* of a field is defined as the number of elements contained in that field. and characteristic p.

Definition 2.2.1 *A field $\mathbb{F}$ has characteristic p if p is the smallest positive integer such that for every nonzero element $a \in \mathbb{F}$, we have $pa = 0$. If no such integer exists, then $\mathbb{F}$ has characteristic 0.*

Given that students should be familiar with prime factorization of compound numbers by this point in the course, it should not be difficult for them to see and prove why this characteristic p must be prime if it is nonzero and if it is indeed the smallest positive integer that gives us $pa = 0$. For example, a compound p would have prime factors such as m and n that would give us $pa = (mn)a = 0$, implying that either $ma = 0$ or $na = 0$, contradicting the assumption that p is the smallest positive integer that gives us this product.

Finite fields are important in the study of elliptic curves and especially elliptic curve cryptography due to the fact that an elliptic curve over a finite field contains a finite number of elements. This will be discussed in more depth in Chapter 3.

2.3 Constructing Tables for the Field $\mathbb{F}_5$

Let us consider a simplistic finite field, $\mathbb{F}_5$, with order $q = 5^1$, giving us the characteristic $p = 5$. Let us assume that the set of elements in $\mathbb{F}_5$ is $\{0, 1, 2, 3, 4\}$, giving us the following addition and multiplication tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 2.3: Addition Table for $\mathbb{F}_5$

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 2.4: Multiplication Table for $\mathbb{F}_5$

We can use this finite field to construct an elliptic curve in Chapter 3, and then later to complete a cryptographical example in Chapter 5.

Chapter 3

Elliptic Curves

3.1 Defining Elliptic Curves over $\mathbb{R}$

First, it is worth noting that elliptic curves have almost nothing to do with ellipses, which would have equations of the form $\left(\frac{x-h}{a}\right)^2 + \left(\frac{y-k}{b}\right)^2 = 1$. Rather, elliptic curves are curves that are naturally a group.

Definition 3.1.1 *An elliptic curves are curves given by equations of the form*

$$y^2 = x^3 + Ax^2 + Bx + C.$$

The cubic part of this equation, $x^3 + Ax^2 + Bx + C$ must have distinct roots, and a discriminant $\Delta = 4\alpha^3 + 27\beta^2$ that is non-zero, where $\alpha = \frac{1}{3}(3B + A^2)$ and $\beta = \frac{1}{27}(2A^3 - 9AB + 27C)$. This gives us the group

$$E = \left(\{(x, y) : y^2 = x^3 + Ax^2 + Bx + C\} \cup \{\mathcal{O}\}, \oplus\right),$$

where $\mathcal{O}$ is defined as a point at infinity, and $\oplus$ is the addition between two given points on an elliptic curve.

The set of solutions (x, y) in a field $\mathbb{F}$ of this elliptic curve, where $A, B,$ and $C \in \mathbb{F}$, along with the additive operation $\oplus$ and a point at infinity $\mathcal{O}$ form the subgroup:

$$E(\mathbb{F}) = (\{(x, y) \in E : x, y \in \mathbb{F}\} \cup \{\mathcal{O}\}, \oplus).$$

Notice that a point at infinity $\mathcal{O}$ is included in the set. The reason for this will become clear when we explain why elliptic curves form groups.

From [She], for a field $\mathbb{F}$ containing either $\mathbb{Q}$ or $\mathbb{F}_p$, such that $p \neq 2, 3$, and p is prime, we can further assume the curve has the form $y^2 = x^3 + \alpha x + \beta$. It is also important to note that elliptic curves whose points are in a finite field $\mathbb{F}_p$ form finite groups. This detail is what makes elliptic curve cryptography possible.

Now, while an introduction to group theory is useful for understanding the finite fields in Chapter 1, it is necessary for students to understand the group axioms before elliptic curves are introduced. For reference, these group axioms, for a nonempty set G and a binary operation $\circ$, are:

1. Identity: There exists an identity element $e \in G$ such that $\forall$g$\in G$, $e \circ g = g \circ e = g$.

2. Inverse: For every element $g \in G$, $\exists$ a unique inverse element $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.

3. Closure: For any two elements $a, b \in G$, $(a \circ b) \in G$.

4. Associativity: For any three elements $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.

For a given elliptic curve E, we denote the addition between two points as $(\oplus)$ and we treat the point at infinity $\mathcal{O}$ as the additive identity. The group axioms then state:

1. $P \oplus \mathcal{O} = P$ $\forall P \in E.$
2. $P \oplus (-P) = \mathcal{O}$ $\forall P, (-P) \in E.$
3. For all $P, Q \in E$, $P \oplus Q \in E.$
4. $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R,$ $\forall P, Q, R \in E.$

Along with these axioms, we can show that E is abelian, i.e. $P \oplus Q = Q \oplus P, \forall P, Q \in E$.

3.1.1 Showing that Elliptic Curves Form an Abelian Group

Above, we defined $\oplus$ as an additive operation, but we did not explain what the sum of two points on a curve actually meant. We define the sum of three aligned, non-zero points on E, as shown in Figure 3.1, to be $P \oplus Q \oplus R = \mathcal{O}$. Since the order of these three aligned points is irrelevant, in that the line L through R, Q, P is the same line through P, Q, R and Q, P, R and the three other permutations of the three points, we can say that this operation is commutative. Because of this, $P \oplus Q = -R$, where $-R$ is a reflection of R over the x-axis. So, for $R = (x, y)$, $-R = (x, -y)$.

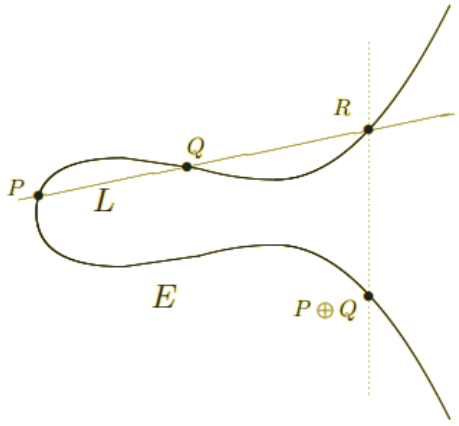

Figure 3.1: Geometrically showing the addition of P, Q, and R, as well as their relationship to the reflected point $P \oplus Q$, on $y^2 = x^3 - 5x + 8$. [Sil]

Since $P \oplus Q \oplus R = \mathcal{O}$ and $P \oplus Q = -R$, $-R \oplus R = \mathcal{O}$. This allows use to define the addition of points on a vertical line, as shown in Figure 3.2.

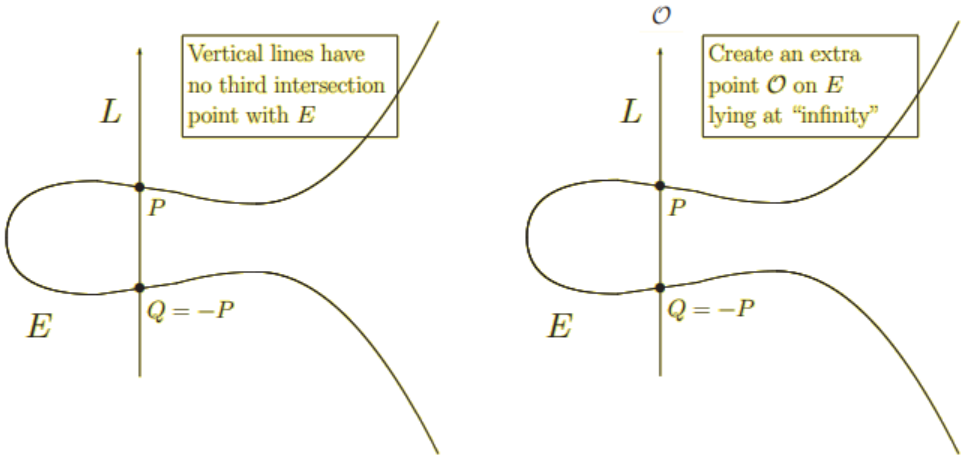

Figure 3.2: Showing the addition of two vertically aligned points on $y^2 = x^3 - 5x + 8$. [Sil]

Since commutativity is not one of the group axioms, it is important to show that the four axioms hold for us to claim that elliptic curves form groups. We will cover a very simplified explanation of how elliptic curves satisfy the group axioms.

Starting with the identity element, since $\mathcal{O} \in E$ and, as established above, $-R \oplus R = \mathcal{O}$, it is implied that $R = \mathcal{O} \oplus R$. Thus there exists an identity element in E.

For the inverse elements, we again consider that $-R \oplus R = (P \oplus Q) \oplus R = \mathcal{O}$. We can see that an inverse exists for a point R, so we must show that this inverse is unique. The first case where we assume that $(P \oplus Q) = -R$ and $(P \oplus Q) = -R'$, where it is initially assumed that $-R \neq -R'$ is fairly trivial and should be easy for students to prove uniqueness by contradiction. To show quickly how this might be approached, if $(P \oplus Q) = -R$ and $(P \oplus Q) = -R'$, then $P \oplus Q \oplus R = \mathcal{O} = P \oplus Q \oplus R'$, which gives us $R = R' \implies -R = -R'$, which contradicts our earlier assumption. The second case for this would be where we consider two lines L_1 and L_2 that both contain R. So $P \oplus Q \oplus R = \mathcal{O}$ and $S \oplus T \oplus R = \mathcal{O}$. Again, it is rather trivial to show that both $P \oplus Q = -R$ and $S \oplus T = -R$, and $P \oplus Q = S \oplus T$, so $-R$ is the unique inverse and reflect point for R.

Proving closure is also trivial, given the innate symmetry of elliptic curves (and not just the one shown) from the y^2 part of the equation. If (x, y) is a solution of $y^2 = x^3 + x + \beta$, then $(x, -y)$ gives us $(-y)^2 = x^3 + \alpha x + \beta \implies y^2 = x^3 + \alpha x + \beta$, implying that (x -y) is also a valid solution. Thus, a point $R \in E$ has a reflected point $P \oplus Q$ that is also in E.

Finally, associativity. Since we defined the additive operation such that $P \oplus Q \oplus R = \mathcal{O}$ and that the operation is commutative, we can first show that $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, and in a second case where, without loss of generality, we let $P = Q$ (the line L is tangent to a point P), that $P \oplus (P \oplus R) = (P \oplus P) \oplus R$.

For the first case, since the operation is commutative, $P \oplus Q \oplus R = Q \oplus R \oplus P$. We know from above that $P \oplus Q = -R$ is true, and it can be shown from $Q \oplus R \oplus P = \mathcal{O}$ that $Q \oplus R = -P$. Thus $(P \oplus Q) \oplus R = -R \oplus R = \mathcal{O} = P \oplus -P = P \oplus (Q \oplus R)$.

For the second case, where we have a point of tangency on a non-vertical line L, $P \oplus P \oplus R = \mathcal{O}$

tells us that $P \oplus P = -R$ and $P \oplus R = -P$. Thus $P \oplus (P \oplus R) = P \oplus -P = \mathcal{O} = -R \oplus R = (P \oplus P) \oplus R$. Therefore, $\oplus$ is an associative operation.

$\therefore$ The four group axioms hold, and $\oplus$ is commutative, so elliptic curves form abelian groups.

Now, these axioms as written aren't helpful in determining R or $-R$, so we looks to the Group Law summary given in [She] that tells us: If, for an elliptic curve $E : y^2 = x^3 + \alpha x + \beta$, if we have points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ such that $P \neq -Q$, then we can determine the third point $R = (x_R, y_R)$ aligned with P and Q using the following equations:

- If $x_P \neq x_Q$, then $m = (y_Q - y_P)(x_Q - x_P)^{-1}$.
- If $x_P = x_Q$, then $m\ (3x_P^2 + \alpha)(2y_P)^{-1}$, where α is the linear coefficient from the elliptic curve equation.
- $x_R = m^2 - x_P - x_Q$
- $y_R = [m(x_R - x_P) + y_P]$, or similarly
- $y_R = [m(x_R - x_Q) + y_Q]$

3.2 Elliptic Curves over Finite Fields

These axioms continue to hold for elliptic curves over finite fields, however the smooth geometric curves illustrated in the above figures are for an elliptic curve over $\mathbb{R}^2$. The plots for an elliptic curve over a finite field maintain the same symmetry over a horizontal line, though it is symmetric over the line $y = p/2$, where p is the characteristic of the polynomial.

Similarly, we can algebraically determine the point that is aligned with two other given points in an elliptic curve. The equations follow from previous section, only requiring the addition of a $\pmod p$ for each item. Thus, for an elliptic curve $E : y^2 = x^3 + \alpha x + \beta$, if we have points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ such that $P \neq -Q$, then we can determine the third point $R = (x_R, y_R)$ aligned with P and Q using the following equations:

- If $x_P \neq x_Q$, then $m = (y_Q - y_P)(x_Q - x_P)^{-1} \pmod p$.
- If $x_P = x_Q$, then $m = (3x_P^2 + \alpha)(2y_P)^{-1} \pmod p$, where α is the linear coefficient from the elliptic curve equation.
- $x_R = [m^2 - x_P - x_Q] \pmod p$
- $y_R = [m(x_R - x_P) + y_P] \pmod p$, or similarly
- $y_R = [m(x_R - x_Q) + y_Q] \pmod p$

Also, using these equations, it is possible to establish definitions for the order and cofactor of a given base point, which are important concepts for Chapters 4 and 5.

Definition 3.2.1 *Since a finite field has a finite characteristic, each point in that field has a finite order. Selecting a point P as our base point, the* order *of P is the number of points P will generate when continuously added to itself. To phrase this another way, the order of P is the smallest integer n such that $nP = P \oplus P \oplus \ldots \cdots \oplus P = \mathcal{O}$.*

Definition 3.2.2 *The* cofactor *of a point P is the order of the entire group (the total number of points on the elliptic curve) divided by the order of P.*

3.3 Example of an Elliptic Curve over $\mathbb{F}_5$

Let $\alpha = 3$ and $\beta = 2$, giving us $E : y^2 = x^3 + 3x + 2$ for our elliptic curve. Since the discriminant $\Delta = 4\alpha^3 + 27\beta^2 = 4(27) + 27(4) = 216 \equiv 1 \pmod 5 \neq 0$, this equation defines an elliptic curve over $\mathbb{F}_5$. Using the addition and multiplication tables we determined at the end of Chapter 2, for each $x \in \mathbb{F}_5$, this gives us

x	y^2	y
0	2	–
1	1	1, 4
2	1	1, 4
3	3	–
4	3	–

Table 3.1: Solutions for $y^2 = x^3 + 3x + 2 \pmod 5$

So $E(\mathbb{F}_5) = \{\mathcal{O}, (1,1), (1,4), (2,1), (2,4)\}$. If we let $P = (1,1)$ and $Q = (2,4)$, we can find the third point R by using the equations listed on page 14. Since P and Q have different x-components, we use the first equation for m,

$$\begin{aligned} m &= (y_Q - y_P)(x_Q - x_P)^{-1} \pmod p \\ &= (4-1)(2-1)^{-1} \pmod 5 \\ &= 3 \pmod 5 \end{aligned}$$

Then, we can determine x_R as

$$\begin{aligned} x_R &= \left[m^2 - x_P - x_Q\right] \pmod p \\ &= \left[3^2 - 1 - 2\right] \pmod 5 \\ &= [6] \pmod 5 \\ &= 1 \pmod 5 \end{aligned}$$

and y_R as

$$\begin{aligned} y_R &= [m\,(x_R - x_P) + y_P] \pmod p \\ &= [3\,(1-1)+1] \pmod 5 \\ &= [3(0)+1] \pmod 5 \\ &= 1 \pmod 5 \end{aligned}$$

Thus, the third point R is actually the point $P = (1, 1)$, making P a point of tangency. This tells us that

$$\begin{aligned} & P \oplus P \oplus Q = \mathcal{O} \\ & \implies 2P = P \oplus P = (-Q) \\ & \implies 3P = P \oplus P \oplus P = (-Q) \oplus P \\ & \implies 4P = P \oplus P \oplus P \oplus P = (-Q) \oplus (P \oplus P) = (-Q) \oplus (-Q) \\ & \dots \\ & \implies 6P = 2(3P) = P \oplus P \oplus P \oplus P \oplus P \oplus P = (-Q) \oplus (-Q) \oplus (-Q) \end{aligned}$$

We could continue this pattern, but given that, including $\mathcal{O}$, there are only five points in $E\,(\mathbb{F}_5)$, we can only generate a finite number of different points before P generates itself. By calculating $2P, 3P$, $4P$, and $6P$ we get

$$\begin{aligned} 2P &= (2, -4) \pmod 5 = (2, 1) \pmod 5 \\ 3P &= (2, -1) \pmod 5 = (2, 4) \pmod 5 \\ 4P &= (1, -1) \pmod 5 = (1, 4) \pmod 5 \\ &\dots \\ 6P &= (1, -4) \pmod 5 = (1, 1) \pmod 5 \end{aligned}$$

Note that $5P$ is omitted from our calculations. This is because, in trying to implement the equations for $5P = 4P + P$ will result in two different points depending on which point, $4P$ or P you choose to use in the equation for m. This is implies that $5P = \mathcal{O}$.
Therefore, we can determine the order of P as $|P| = 5$, and the cofactor of P is 1, since the order of $E\,(\mathbb{F}_5)$ is 5, and $5/5 = 1$.

Chapter 4

Cryptography

4.1 Definition of Cryptography

To put it simply, cryptography is the art and science of writing and solving codes and cipher systems. In this day and age of technology, we do nearly everything online, from our holiday shopping to checking our bank account balances. This has made the study of cryptography invaluable to ensuring that our personal information and finances are secure while we continue to exist in such a technologically connected environment.

In this chapter, we will briefly cover the basics of the RSA Algorithm, the Diffie Hellman Public-Key Algorithm and ElGamal Encryption, and the Diffie-Hellman and ElGamal analogues using elliptic curves.

4.2 RSA Algorithm

To begin, RSA stands for Rivest-Shamir-Adleman, which are the surnames of the individuals who first were able to publicly develop and describe the algorithm. It was one of the first public-key algorithms to be developed. It is generally used for secure data transmission, as we will demonstrate below.

To encrypt a message using RSA, it is first necessary to convert the literal plaintext of the message into a numerical plaintext integer or groups of integers, which we will refer to as M. Next, we choose two large prime numbers, p and q, and let $n = pq$ and $\phi(n) = (p-1)(q-1)$. Lastly, we choose a value j such that $gcd(j, \phi(n)) = 1$.

Then, we can encipher our message M by

$$M^j \equiv C \pmod{n},$$

which yields the numerical ciphertext message C.

In order to decipher this text to determine the original message, it is necessary to know the integer k such that $jk \equiv 1 \pmod{\phi(n)}$. Because of Fermat's Little Theorem, as mentioned in Chapter 1, we can decipher C as

$$C^k \equiv \left(M^j\right)^k \pmod{n} \equiv M \pmod{n},$$

giving us the original numerical plaintext message, M.

4.3 Diffie-Hellman Public-Key Algorithm

This method allows for two or more individuals or entities to securely develop and exchange cryptographic keys over a public channel. Along with the ElGamal encryption, which is discussed in the next subsection, it can be used to send secure encrypted messages. However, its primary purpose is to establish a secure key between entities.

For this explanation of the algorithm, we will call our two entities "Chris" and "Jesse" so the two are clearly distinct.

First, either Chris or Jesse chooses a prime number, p. Preferably, the chosen p is very large. Also chosen is a number $q \in U_p$ where U_p is the group of units $(\mathrm{mod}\ p)$, and such that the order of q is also large. Preferably, q is a primitive root of U_p. These numbers are shared between Chris and Jesse.

Chris then chooses an integer a such that $1 < a < p-1$ is true and computes $q^a \equiv C\ (\mathrm{mod}\ p)$.

Similarly, Jesse chooses an integer b such that $1 < b < p-1$ is also true and computes $q^b \equiv J\ (\mathrm{mod}\ p)$. Then, Chris and Jesse publicly exchange C and J.

Chris now computes $J^a \equiv \left(q^b\right)^a\ (\mathrm{mod}\ p)$ and Jesse computes $C^b \equiv \left(q^a\right)^b\ (\mathrm{mod}\ p)$. Both now possess a key $q^{ab}\ (\mathrm{mod}\ p)$ that would be rather difficult for anyone else intercepting their messages to obtain.

4.3.1 ElGamal Encryption

This encryption method is very similar to the Diffie-Hellman in regards to what information is public and what is private. The most notable difference is the addition of a message. So, if Jesse wishes to send Chris a message that has been converted to a numerical equivalent integer M, the exchange would differ slightly.

Using the information from the Diffie-Hellman Algorithm, Chris would still choose a number a such that $1 < a < p-1$ is true and compute $q^a \equiv C\ (\mathrm{mod}\ p)$. Then C is shared with Jesse.

Jesse would also still choose a number b such that $1 < b < p-1$ is true and compute $q^b \equiv J\ (\mathrm{mod}\ p)$. However, Jesse would also compute $M * (C)^b \equiv K\ (\mathrm{mod}\ p)$ using Chris's public C. Jesse would then share the ordered pair (J, K).

Using a and J, Chris can now compute $J^a \equiv C^b\ (\mathrm{mod}\ p) \equiv q^{ab}\ (\mathrm{mod}\ p)$. Then, by determining the inverse of $q^{ab}\ (\mathrm{mod}\ p)$ as $q^{p-1-ab}\ (\mathrm{mod}\ p)$, Chris can compute $K * q^{p-1-ab} \equiv M\ (\mathrm{mod}\ p)$ to retrieve the message M.

4.4 Elliptic Curve Cryptography (ECC)

Using elliptic curves, we can also encrypt plaintext by embedding it into a point or set of points in an elliptic curve. We can also create analogues to the Diffie-Hellman Public-Key Algorithm and ElGamal encryption method by using elliptic curves.

Similar to what we described in the RSA section, to encipher plaintext we must first convert this plaintext into a numerical plaintext integer, $m \geq 0$. For an elliptic curve over a finite field $\mathbb{F}_{p^k}$, we choose a parameter n such that the probability of failing to embed the plaintext into E is less than

2^{-n} . For the sake of this explanation, we will consider n to be a predetermined parameter. Now, we need $mn < p$. Otherwise, we need to package the message m into blocks of smaller-degree integers, m_i such that each $m_i < p$. This method of repackaging demonstrates another measure of usefulness of a large prime number P.

Satisfying this, we then find a solution (x, y) on our elliptic curve $\pmod p$, such that $mn < x < (m+1)n$. This point (x, y) is then our embedded version of the message m.

To decipher m, we start by knowing that $mn \leq x < (m+1)n$ the point (x, y). From this, we see that

$$mn \leq x < (m+1)n \implies m \leq \frac{x}{n} < m+1$$

Since m is an integer, $m = \left\lfloor \frac{x}{n} \right\rfloor$ recovers the original numerical plaintext integer, from which we can extract the original literal plaintext of the message.

4.4.1 Elliptic Curve Diffie-Hellman (ECDH)

In the section explaining the Diffie-Hellman Algorithm, the two entities had to choose a prime number p and a number $g \in U_p$, preferably so that g is a primitive root of U_p. For Elliptic Curve Diffie-Hellman, or ECDH, the choice becomes easier, as one of the two entities needs to choose a prime number p, then $\alpha, \beta \in \mathbb{F}_p$ to construct $E : y^2 = x^3 + \alpha x + \beta$. So for ECDH, $E(\mathbb{F}_p)$ replaces the need for U_p. Then, in place of q, a basepoint $G \in E(\mathbb{F}_p)$ is chosen. It is recommended that a basepoint is chosen such that its order, $|G|$, is large .

Following our explanation of the Diffie-Hellman Algorithm, let us use Chris and Jesse again here. Chris will choose a random integer a such that now $1 < a < |G|$, and compute aG, where aG is the point G added to itself a number of times using the equations from Chapter 3.
Similarly, Jesse will choose a random integer b such that $1 < b < |G|$ and compute bG. Chris and Jesse then publicly exchange points aG and bG, allowing both to compute $a(bG) = b(aG)$ as their shared secret key.

This can also be used to create an analogue of the ElGamal Encryption by combining the plaintext encryption to embedded a message into a point P_m and the ECDH, so that Jesse instead uses Chris's public point aG, chooses a random integer b such that $1 < b < |G|$, and shares the ordered pair $(bG, P_m \oplus b(aG))$ with Chris. Chris can then compute $a(bG)$ using Jesse's public point and uses this to determine $-a(bG) = -b(aG)$. Chris can then extract the message P_m by solving $(P_m \oplus b(aG)) \oplus -b(aG) = P_m$. Finally, the literal plaintext message can be decrypted from P_m.

Chapter 5

Example

5.1 The Exercise

To compare the Elliptic Curve Diffie-Hellman Analogue with the Diffie-Hellman Method itself, we chose a small, manageable prime number for p. For both methods, we let $p = 5$. To avoid confusing students and over-complicating the example, we will not encrypt a plaintext message here.

5.2 Using the Diffie-Hellman Method

Let $q = 3$ for this example. Again using our characters, Chris and Jesse, we have Chris and Jesse choose integers between 1 and $5 - 1$. We will let Chris choose $a = 2$ and Jesse choose $b = 3$.

Chris then computes $q^a = 3^2 \equiv 4 \pmod 5$. So $C = 4$. Jesse then computes $q^b = 3^3 \equiv 2 \pmod 5$. So $J = 2$. They both publicly exchange these keys.

Chris now computes $J^a = 2^2 \equiv 4 \pmod 5$, and Jesse computes $C^b = 4^3 \equiv 4 \pmod 5$. So their shared private key is 4.

Given the small prime value we used here, this key would not actually be secure, which is why it is highly recommended that prime numbers with 100 digits or more be used.

5.3 Using the ECDH Method

Recall that in Chapters 2 and 3, we established $\mathbb{F}_5$ and found the set of points on the elliptic curve $y^2 = x^3 + 3x + 2$ over this finite field to be $E(\mathbb{F}_5) = \{\mathcal{O}, (1,1), (1,4), (2,1), (2,4)\}$. Since we intend to choose a basepoint and add it to itself for this method, we will need the following equations from Chapter 3:

- If $x_P \neq x_G$, then $m = (y_G - y_P)(x_G - x_P)^{-1} \pmod 5$.
- If $x_P = x_G$, then $m = (3x_G^2 + 3)(2y_G)^{-1} \pmod 5$
- $x_R = [m^2 - x_P - x_G] \pmod 5$
- $y_R = [m(x_R - x_G) + y_G] \pmod 5$

In Chapter 3, we found the order of P to be 5, so let us set our basepoint, G, as $(1,1)$. Then, we will let Chris choose $a = 2$ and Jesse choose $b = 4$. Using our calculations from Chapter 3, Chris computes $aG = 2G = (2,1)$. Jesse then computes $bG = 4G = (1,4)$. Chris and Jesse then exchange their points, $aG = (2,1)$ and $bG = (1,4)$. From this point, both Chris and Jesse are able to compute $abG = 8G = 3G \pmod 5 = (2,4)$ as the "secret" key.

While this example was relatively rudimentary, it establishes the necessary steps for the algorithm concisely enough so students would understand the concept in a short amount of classroom

time. Also, using a finite field with even just 7, 11, or even 3^2 elements would greatly improve the security of this method. Provided below are the multiplication tables for $(F)_7$ and $(F)_{11}$.

$*$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 5.1: Multiplication Table for $\mathbb{F}_7$

$*$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Table 5.2: Multiplication Table for $\mathbb{F}_{11}$

Also, we include addition and multiplication tables for $(F)_{3^2}$, as students may not readily see that $(F)_{3^2} = (F)_3/ < x^2 + 1 >$, using the same techniques outlined in the example in Chapter 2.1.1.

$+$	0	1	2	a	$2a$	$1+a$	$1+2a$	$2+a$	$2+2a$
0	0	1	2	a	$2a$	$1+a$	$1+2a$	$2+a$	$2+2a$
1	1	2	0	$1+a$	$1+2a$	$2+a$	$2+2a$	a	$2a$
2	2	0	1	$2+a$	$2+2a$	a	$2a$	$1+a$	$1+2a$
a	a	$1+a$	$2+a$	$2a$	0	$1+2a$	1	$2+2a$	2
$2a$	$2a$	$1+2a$	$2+2a$	0	a	1	$1+a$	2	$2+a$
$1+a$	$1+a$	$2+a$	a	$1+2a$	1	$2+2a$	2	$2a$	0
$1+2a$	$1+2a$	$2+2a$	$2a$	1	$1+a$	2	$2+a$	0	a
$2+a$	$2+a$	a	$1+a$	$2+2a$	2	$2a$	0	$1+2a$	1
$2+2a$	$2+2a$	$2a$	$1+2a$	2	$2+a$	0	a	1	$1+a$

Table 5.3: Addition Table for $\mathbb{F}_{3^2}$

$*$	0	1	2	a	$2a$	$1+a$	$1+2a$	$2+a$	$2+2a$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	a	$2a$	$1+a$	$1+2a$	$2+a$	$2+2a$
2	0	2	1	$2a$	a	$2+2a$	$2+a$	$1+2a$	$1+a$
a	0	a	$2a$	2	1	$2+a$	$1+a$	$2+2a$	$1+2a$
$2a$	0	$2a$	a	1	2	$2+2a$	$1+2a$	$1+a$	$2+a$
$1+a$	0	$1+a$	$2+2a$	$2+a$	$1+2a$	$2a$	2	1	a
$1+2a$	0	$1+2a$	$2+a$	$1+a$	$2+2a$	2	a	$2a$	1
$2+a$	0	$2+a$	$1+2a$	$2+2a$	$2+a$	1	$2a$	a	2
$2+2a$	0	$2+2a$	$1+a$	$1+2a$	$2+a$	a	1	2	$2a$

Table 5.4: Multiplication Table for $\mathbb{F}_{3^2}$

Using these tables, students should be able to determine the set of points on an elliptic curve over each field. From there, they can use these points to implement the Elliptic Curve Diffie-Hellman Algorithm between two entities.

Bibliography

[Bab] L. Babinkostova, *Embedding Plaintext into an Elliptic Curve Group*, Boise State University, 2018 http://diamond.boisestate.edu/∼liljanab/MATH308/ECembed.htm Last accessed 6 Apr 2018.

[Jud] T. W. Judson, *Abstract Algebra: Theory and Applications*, 210–283, Orthogonal Publishing, 5 Aug 2017, http://abstract.ups.edu/download/aata-20170805.pdf.

[Mil] S. J. Miller R. Takloo-Bighash, *An Invitation to Modern Number Theory*, 85–89, Princeton University Press, 2006.

[Rob] N. Robbins, *Beginning Number Theory, Second Edition*, 305–311, Jones and Bartlett Publishers, 2006.

[She] T. R. Shemanske, *Modern Cryptography and Elliptic Curves: A Beginner's Guide*, Student Mathematical Library, 83, American Mathematical Society, 2017.

[Sil] J. H. Silverman, *An Introduction to the Theory of Elliptic Curves*, Brown University, 2006, https://www.math.brown.edu/∼jhs/Presentations/WyomingEllipticCurve.pdf, Last accessed 6 Apr 2018.

Academic Vita

Lauren Jeanette Minner
ljm5281@psu.edu

Education

The Pennsylvania State University, Behrend Campus

- 2014 - 2018
- Bachelor of Science, Mathematics
  - Minor: Physics
- Schreyer Scholar

Research

Examining the Methods of Partial Fraction Decomposition with Dr. Antonella Cupillari (Penn State Erie). August 2016 February 2017

- Presented research at Sigma Xi Conference hosted by Penn State Behrend, April 22, 2017

Increasing the Area of a White Scattering Background can Increase the Power Output of a Luminescent Solar Concentrator with Dr. Bruce Wittmershaus (Penn State Erie), Jonathon R. Schrecengost, Seth D. Bowser, Seth W. Weible, Joel M. Solomon, Jesse T. Gresh. May 2016 August 2016

- Submitted for review and future publication

Mathematical Arachnology: A Preliminary Study with Dr. Daniel Joseph Galiffa (Penn State Erie). January 2016 April 2016

- Presented research at:
  - Penn State Behrend Math Club Speaker Series, October 27, 2017
  - Math Options Program, May 10, 2016;
  - 21st Century Kids Program, April 26, 2016;
  - MAA Allegheny Mountain Section Meeting April 1, 2016;

The Discrete Sheffer Sequences and Schrodinger Form with Dr. Daniel Joseph

Galiffa (Penn State Erie), Mrs. Jennifer K. Ulrich (Penn State Erie), and Derek J. Shaffer. February 2015 February 2016.

- Submitted and approved for review and future publication
- Presented research at:
  - Sigma Xi Conference hosted by Penn State Behrend, April 16 2016
  - Pi Mu Epsilon Ohio Chapter Meeting at Youngstown State University, February 20, 2016

Barcoding of Behrend with Dr. Matthew E. Gruwell (Penn State Erie) and Kyler Miller. August 2014 January 2015.

Employment

August, 2016 Present

Higher Education Mathematics Intern for Larson Texts Inc.

- Tutors students ranging from Middle School to College Calculus and Linear Algebra
- Communicates ideas effectively through CalcChat and Big Ideas Math web clients
- Creates ancillary keys and solutions for textbook problems.
- Proofreads and edits ancillary keys and solutions for textbook problems and supplementary student materials.

May 2015 August, 2016:

Tutor for Penn State Behrend's Learning Resource Center

- Classes Tutored: Math 110, 140, 141, 220, 230, 251, 311, 455, 456, and Prealgebra and Precalculus Courses, Stat 200, 301, 401, Phys 250, 251, 211, 212

June 2016 August 2016

Undergraduate Research Assistant

- Luminescent Solar Concentrators with Dr. Wittmershaus; NSF Sponsored

August 2015 May 2016:

Teaching Assistant for Phys 211 Class

- Assisted students in class during lecture and group activities
- Graded quizzes and assignments
- Held weekly Study Sessions for students in need of further help

August 2015 December 2015:

Grader for the Mathematics Department, specifically for Dr. Galiffa

- Graded quizzes and assignments

Volunteer Work

Science Olympiad: March 6, 2018

- Judge for Division C Anatomy Physiology

Science Olympiad: March 7, 2017

- Judge for Division C Optics with Mr. Jonathan Hall

Math Options for Girls Workshop: May 10, 2016

- Event: Mathematical Arachnology: Probability and Genetics

21st Century Kids Workshop: April 26, 2016

- Event: Mathematical Arachnology: Probability and Genetics

Science Olympiad: March 7, 2016

- Judge for Division C Geologic Mapping with Dr. Amos Ong

Physics Day: November 24, 2015

- Assisted Dr. Chuck Yeung and Dr. Darren Williams with Physics Jeopardy Activity

Math Options for Girls Workshop: May 12, 2015

- Event: Critical Thinking

Science Olympiad: March 10, 2015

- Supervised Impound for Air Trajectory Event
- Judge for Division C Entomology Event with Dr. Matthew E. Gruwell

Awards

August 2017:

- Awarded a School of Science Scholarship March 26, 2017
- Inducted as a member of the Honor Society of Phi Kappa Phi

August 2016:

- Awarded a School of Science Scholarship

April 17, 2016:

- Awarded the Mathematics Competition Scholarship Award
- Awarded the Honors Certificate for meeting the requirements of the Penn State Behrend Honors Program

April 2016 Present:

- Member of the Pi Mu Epsilon National Mathematics Honors Society: Pi Mu Epsilon Pennsylvania Alpha Beta Chapter
  - President as of April 2017
  - Treasurer as of April 2016

August 2015 Present:

- Member of Behrend Math Club
  - President as of May 2017
  - Treasurer as of May 2016

April 19, 2015:

- Awarded the Most Promising Freshman in Mathematics