The Report Committee for Crystal Dawn Jensen
Certifies that this is the approved version of the following report:

Elliptic Curves

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: Efraim Armendariz

Co-Supervisor: Mark Daniels

Elliptic Curves

by

Crystal Dawn Jensen, BS

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Arts

The University of Texas at Austin

August 2010

Abstract

Elliptic Curves

Crystal Dawn Jensen, MA

The University of Texas at Austin, 2010

Supervisors: Efraim Armendariz and Mark Daniels

This report discusses the history, use, and future of elliptic curves. Uses of elliptic curves in various number theory settings are presented. Fermat's Last Proof is shown to be proven with elliptic curves. Finally, the future of elliptic curves with respect to cryptography and primality is shown.

Table of Contents

List of Figures

Chapter 1: An Introduction

Elliptic curves have been studied and developed largely in the last century. These curves first emerged in the study of arc lengths of ellipses and circles. The elliptic curve is an equation that can be used to find the arc length of these conic sections. Further applications of these relationships have shown that elliptic curves are closely tied to Pythagorean topics: triples, rational right triangles, and congruent numbers.

Elliptic curves provide *congruent numbers*. A congruent number is one that is the area of a right triangle with rational sides. One can use elliptic curves to find these types of numbers, and to find the sides that make these right triangles. Surprisingly, elliptic curves have also been used to show that for every congruent number there are infinitely many dissimilar rational right triangles with the given area [**4**].

Elliptic curve theory has also been used to prove several theorems from number theory. One theorem, discussed later in this report, shows that a triangle can only be divided into five or more rational right triangles; however, the most prominent use of elliptic curves was to solve one of the most famous problems in number theory history, Fermat's Last Theorem. According to Brown, Wiles used elliptic curves to finally prove the theorem that had been unsolved for hundreds of years [**3**]. This mathematical feat is why the author chose the study of elliptic curves. Elliptic curves and all their accompanying algebra and theory were mostly developed in the last century. It is interesting to note that the mathematics needed to solve a problem, probably written in 1637, were to be discovered and developed in this century even though Fermat himself noted that he had a proof for his Last Theorem in his copy of Diophantus' *Arithmetica* [**3**, p. 170]. Some mathematicians speculate whether he truly had a proof for this theorem [**4**, p. 309].

Since the proof of Fermat's Last Theorem, elliptic curves have been brought into modern times. Now, they are used to generate and verify primality of numbers for cryptography [**1**]. This path from Fermat to modern technology and secrecy is an interesting course for any mathematics topic.

In the following, elliptic curves are explored beginning with their origins and algebra. Subsequently, some applications and number theory problems are discussed.

Chapter 2: Origins of Elliptic Curves

A circle that is centered at the origin and with a radius of *r* has the formula $x^2 + y^2 = r^2$. Consider the circle with radius one and centered at the origin, namely $x^2 + y^2 = 1$. In order to find the area or the arc length of this circle, one must evaluate a definite integral involving the equation of a circle, solved for *y* such that $y = \sqrt{1 - x^2}$. This circle can be parameterized by rational equations, namely $x = \frac{1 - t^2}{1 + t^2}$, $y = \frac{2t}{1 + t^2}$. This allows for the integral involving $\sqrt{1 - x^2}$ to be rationalized and solved. However, finding the area and arc length of ellipses is more difficult. An ellipse cannot be parameterized by rational equations, so the integral $u = \int \frac{dx}{\sqrt{x^3 + ax + b}}$ is difficult to solve [**2**]. Instead, let $u = g^{-1}(x)$ and elect to study the inverse of the integral. Since $g(u) = x$,

$$g'(u) = \frac{dx}{du} = \frac{1}{du/dx} = \frac{1}{1/\sqrt{x^3 + ax + b}} = \sqrt{x^3 + ax + b} = y .$$

Then

$$y^2 = x^3 + ax + b$$

became an equation of interest [**7**, p. 836]. Because these types of equations arose from the problem of finding arc lengths and areas of ellipses, they are named elliptic curves.

Chapter 3: Algebra of Elliptic Curves

Finding rational points on an elliptic curve involves geometric ideas. First, a chord is drawn through two known rational points, *A* and *B*. The chord intersects the elliptic curve in a third point, defined as *A*B*. Then, the point *A+B* is the reflection of *A*B* across the *x*-axis. Another method of finding rational points involves using a tangent line to a point on the curve, *A*. The tangent line will intersect the curve at *A*A*, and the reflection of *A*A* is *A+A*, or *2A*. In order to preserve the properties of an Abelian Group for all the rational points on an elliptic curve, the "point at infinity" ***O*** is defined to be the point at either end of a vertical line [**4** pp. 311-312]. ***O*** is included as a point on every elliptic curve. *A+B* and *A*B* are collinear with ***O*** on every elliptic curve.

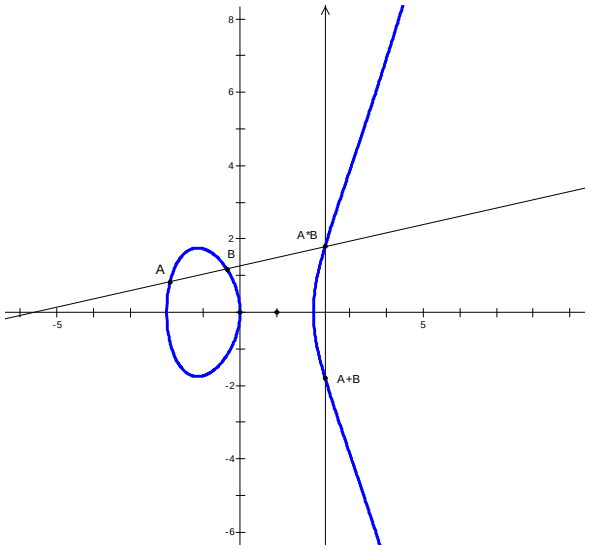

Figure 1. Elliptic Curve Algebra for $y^2 = x^3 - 4x$

Diophantus was the first known mathematician to use the chord/tangent method to find rational points [**7**, p. 832]. He used lines through "obvious" solutions to various

equations to find new points. This method of "adding" rational points to an elliptic curve has allowed several number theory problems to be successfully solved and proven. The following are some examples of the use of elliptic curves to solve interesting problems.

Chapter 4: Making Squares from Pythagorean Triangles

Consider a square with rational sides. Jepsen and Yang proved that such a square can be divided into m Pythagorean triangles if and only if $m \geq 5$ [**5**]. First, a square is divided into 4 triangles with rational sides. Three are right triangles, while the middle triangle, T, is not.

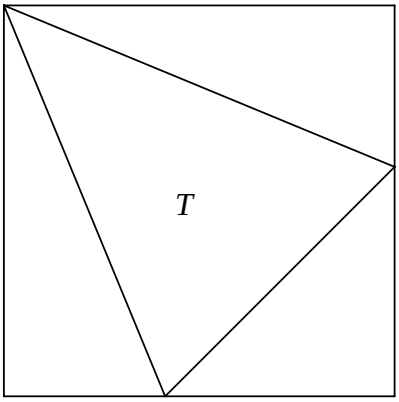

Figure 2. A square dissected into 4 right triangles [**5**, p. 285].

Next, T is divided into two new triangles by drawing the altitude. Thus T has been divided into two right triangles, and the square now contains five such triangles. Using the following figure, some calculations are needed to ensure that the two new triangles formed from T have rational sides.

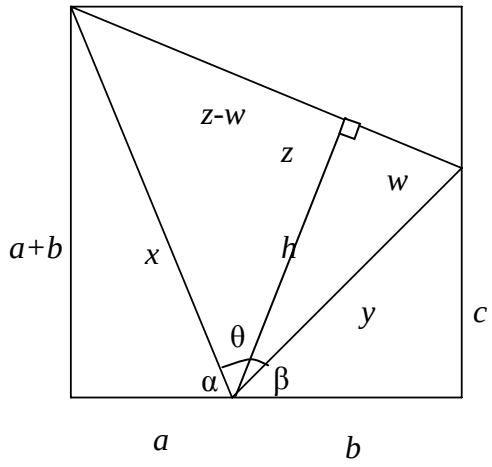

Figure 3. Five right triangles [**5**, p. 285].

First, the area of T is found to be $\frac{1}{2}xy\sin\theta$. Since $\theta = \pi - \alpha - \beta$ and the sine function is odd,

$$\sin\theta = \sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta .$$

This yields

$$\sin\theta = \left(\frac{a+b}{x}\right)\left(\frac{b}{y}\right) + \left(\frac{a}{x}\right)\left(\frac{c}{y}\right) = \frac{b(a+b)+ac}{xy} .$$

Thus the area of triangle T is $\frac{1}{2}xy\left(\frac{b(a+b)+ac}{xy}\right)$, which is

$$\frac{1}{2}(b(a+b)+ac). \qquad (1)$$

The area of *T* is also given by $\frac{1}{2}hz$. Setting this equal to (1), we have

$$h = \frac{b(a+b)+ac}{z}.$$

Since a, b, c, z are all rational, *h* is also rational. Using the Pythagorean Theorem, it is shown that

$$h^2 + w^2 = y^2, \tag{2}$$

and

$$h^2 + (z-w)^2 = x^2, \tag{3}$$

Solving (2) for w^2 and substituting (3) into the equation yields the result

$$w^2 = y^2 - x^2 + (z-w)^2 = y^2 - x^2 + z^2 - 2zw + w^2 \ .$$

Solving this equation for *w*,

$$w = \frac{y^2 - x^2 + z^2}{2z},$$

which is also rational. Finally, since *z* and *w* are rational, *z*-*w* is rational.

Last, Pythagorean triangles need integer sides. Multiplying all sides of the figure by an appropriate integer will yield integral answers, and thus five Pythagorean triangles

have been created inside a square. To create more than five Pythagorean triangles, it is noted that any Pythagorean triangle can be cut into two Pythagorean triangles [**5**].

To prove the converse, an attempt to divide a square into four Pythagorean triangles is made. First, a lemma:

> *If x and y are legs of a Pythagorean triangle, and* $\frac{m}{n} = \frac{x}{y}$, *then m and n are also legs of a Pythagorean triangle* [**5**, p. 286].

If $\frac{x}{y} = \frac{p}{q}$, then $x = pd$ and $y = qd$ for some real number d. Since x and y are sides of a Pythagorean triangle,

$$(pd)^2 + (qd)^2 = z^2 \text{ and } d^2(p^2 + q^2) = z^2.$$

Therefore, d divides z. Let $m = pt$ and $n = qt$ for some real number t, so

$$m^2 + n^2 = (p^2 + q^2)t^2 = \left(\frac{z}{d}t\right)^2.$$

This lemma shows that once a Pythagorean triple (x, y, z) is found, any multiple of the triple, (ax, ay, az) also gives the sides of a right triangle. For the new triple to describe a Pythagorean triangle, a must be an integer.

In order to divide a square into four right triangles, it is necessary that the pairs $(a,\ a+b)$ and $(b,\ a+b)$ be legs of a right triangle.

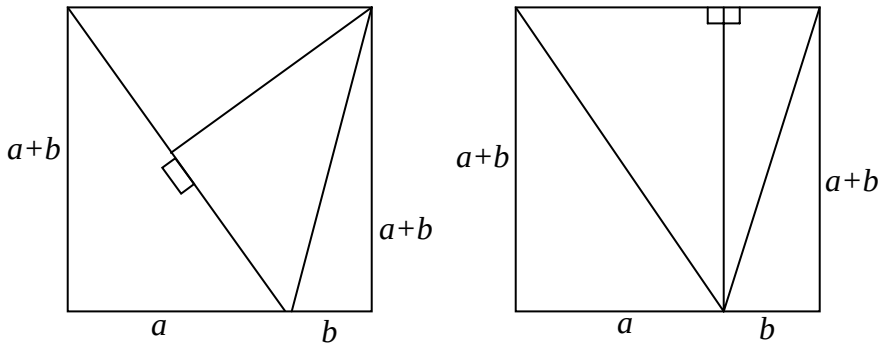

Figure 4. *Possible squares with four right triangles* [**5**, p. 286].

To shorten the search, if *a* and *b* are relatively prime, then one is only looking for *primitive* Pythagorean triples. A triple (a,b,c) is called primitive if $GCD(a,b,c)=1$. First, assume that the pairs are legs of right triangles. Then the set of Diophantine equations

$$\begin{cases} a^2+(a+b)^2=m^2, \\ b^2+(a+b)^2=n^2, \end{cases} \tag{4}$$

arise. Since *a* and *b* are relatively prime, *a*, *b*, *m*, and *n* must be odd. Doubling the top equation of (4) and solving for *b* yields the result

$$b=\frac{2m^2-n^2-3a^2}{2a}.$$

By substituting this into the first equation of (4) one acquires

$$m^2=a^2+\left(a^2+\frac{2m^2-n^2-3a^2}{2a}\right)^2,$$

which through some simplification yields

$$4m^4 + n^4 + 5a^4 - 4m^2n^2 - 8m^2a^2 + 2n^2a^2 = 0.$$

This can be written as

$$\left[\frac{1}{2}\left(n^2 + a^2\right)\right]^2 + \left(m^2 - a^2\right)^2 = \left(mn\right)^2. \tag{5}$$

Since *a* and *b* are relatively prime, the three elements of (5) also have no common factors. So, we have formed a primitive Pythagorean triple such that $m^2 - a^2$ is even. Using Euclid's work [**3**, p. 168], there exist relatively prime positive integers *k* and *l*, $k > l$, with opposite parity, so that

$$\begin{cases} \frac{1}{2}\left(n^2 + a^2\right) = k^2 - l^2, \\ m^2 - a^2 \quad = 2kl, \\ mn \qquad = k^2 + l^2. \end{cases} \tag{6}$$

These equations will surface again later, when congruent numbers are studied. Using the equations from (6), solutions are

$$\begin{cases} \left(m+2\right)^2 = 4k^2 + 2kl, \\ \left(m-n\right)^2 = 2kl - 4l^2. \end{cases} \tag{7}$$

Dividing the first expression by the second expression and letting $x = 2\left(\frac{k}{l}\right)$ yields

$$\left(\frac{m+2}{m-n}\right)^2 = \frac{2\frac{k}{l}+1}{1-2\frac{l}{k}} = \frac{x(x+1)(x-4)}{(x-4)^2}.$$

If $y = \left(\frac{m+n}{m-n}\right)(x-4)$, then our equation becomes $y^2 = x(x+1)(x-4)$, which is an elliptic curve. If there exists a rational solution, (x, y) on the curve, then this implies integer solutions to equations (4). However, this curve only has solutions of (-1, 0), (-2, 0), (3, 0), and **O** (the point at infinity). Since $y = 0$ for these rational solutions, there are no non-trivial solutions to equations (4). Therefore there are no rational numbers a and b such that $(a, a+b)$ and $(b, a+b)$ form the legs of a right triangle. Hence, a square cannot be divided into four Pythagorean triangles.

Questions about triangles in squares have been asked and answered previously, and now the question of how many Pythagorean triangles may be formed inside a square has been settled by the use of elliptic curves.

Chapter 5: Congruent Numbers and Elliptic Curves

Using equations (4) and the rational solutions of elliptic curves to solve problems involving right triangles has also been applied to questions about congruent numbers. Fibonacci found the smallest congruent number, 5 [**4**, p. 308]. Fermat proved that the difference of two fourth powers is never a square. Using this, we can see that the area of a rational right triangle is never a square [**3**]. Then the goal becomes finding which numbers are congruent using an algorithm instead of trying to produce a rational right triangle with specified area. Mathematicians have used elliptic curves to find natural numbers that are congruent and to verify that numbers are congruent.

First, we explore Euclid's method of finding congruent numbers. "Squarefree" congruent numbers—that is, numbers that do not have any square factors, are desired. If two triangles are similar, then their sides are proportional. If the constant of proportionality is c, then the ratio of the areas of the similar triangles is c^2. The general case, then, is to consider the problem for natural numbers having no square factors larger than 1 [**4**].

As mentioned before, Euclid characterized all integral right triangles with sides x, y, and z with $\gcd(x, y, z) = 1$ using the form

$$x = r^2 - s^2,\ y = 2rs,\ z = r^2 + s^2,$$

where r and s are relatively prime integers with opposite parity [**3**]. The method is to find an odd natural number, k, and list all products $rs(r^2 - s^2)$ with $r + s = k$. If $rs\left(r^2 - s^2\right)$ is divisible by m^2, then $rs\left(r^2 - s^2\right) = m^2 n$ for some squarefree n. Because $rs\left(r^2 - s^2\right)$ is the area of the original triangle being considered, m^2 is the constant of proportionality between the areas of the original triangle and the triangle characterized by

$$\left\{\frac{\left(r^2 - s^2\right)}{m}, \frac{2rs}{m}, \frac{\left(r^2 + s^2\right)}{m}\right\}.$$

This new characterization gives a rational right triangle with area n [**3**, p. 168].

However, elliptic curves have shown to be more effective and efficient at finding and verifying congruent numbers. First, the following Diophantine equations must be considered:

$$\begin{cases} x^2 + ay^2 = z^2 \\ x^2 - ay^2 = t^2. \end{cases} \tag{7}$$

Chahal proves that a positive integer a is a congruent number if and only if the system of simultaneous equations in (7) has a non-trivial solution [**4**]. First it is assumed that the system is solvable in integers. Subtracting the equations in (7), one can see that

$$a = \frac{1}{2}\left(\frac{z+t}{y}\right)\left(\frac{z-t}{y}\right).$$

Letting $r = \frac{z+t}{y}$ and $s = \frac{z-t}{y}$, the sides of the triangle in question are clearly rational.

We now need to ensure that $r^2 + s^2 = \left(\frac{z+t}{y}\right)^2 + \left(\frac{z-t}{y}\right)^2 = h^2$ for some *h* that is rational.

If the equations in (7) are added, one obtains $2x^2 = z^2 + t^2$. From above,

$$r^2 + s^2 = \frac{2\left(z^2 + t^2\right)}{y^2} = \frac{2\left(2x^2\right)}{y^2} = \left(\frac{2x}{y}\right)^2 = h^2,$$

and so *h* is rational. The converse is easily shown.

Now that it has been established that if (7) is solvable in the integers then *a* is a congruent number, one equation is needed that will both verify and produce congruent numbers. Using the fact that

$$r^2 + s^2 = h^2 \tag{8}$$

and

$$a = \frac{1}{2}rs, \tag{9}$$

multiply (9) by 4 and add (8) and (9) together. This produces $(r+s)^2 = h^2 + 4a$. Subtracting, the result is $(r-s)^2 = h^2 - 4a$. Dividing the new equations by 4 and then multiplying them together, the result is $\left(\frac{r^2 - s^2}{4}\right) = \left(\frac{h}{2}\right)^4 - a^2$. With a change of variables, let $v = \frac{r^2 - s^2}{4}$ and $u = \frac{h}{2}$. Thus if a is a congruent number, then it produces a rational solution to an equation of the form

$$v^2 = u^4 - a^2. \tag{10}$$

Finally, if (10) is multiplied through by u^2, it becomes $u^2v^2 = u^4u^2 - a^2u^2$. Now, the equation is

$$(uv)^2 = (u^2)^3 - a^2u^2.$$

Let $y = uv$ and $x = u^2$, and finally an elliptic curve emerges:

$$y^2 = x^3 - a^2x. \tag{11}$$

Thus if a is a congruent number, then it produces a rational solution on the elliptic curve (11).

Chahal takes this statement further by proposing the theorem

> *"A square-free integer $a > 0$ is a congruent number if and only if the elliptic curve defined by (11) has infinitely many rational points"* [**4**, p. 311].

Let $E(\mathbb{Q})$ be the set of rational points on any elliptic curve E. Since points on E are finitely generated, then $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where T is a torsion subgroup of $E(\mathbb{Q})$ and consists of the elements of $E(\mathbb{Q})$ of finite order. The Mordell-Weil rank of $E(\mathbb{Q})$ is a non-negative integer, r. Denoted $r_{\mathbb{Q}}(E)$, it is greater than zero if and only if E has infinitely many rational points.

First, suppose that a is a congruent number. Multiplying the equations in (7), $x^4 - a^2y^2 = z^2t^2$. Then, multiplying through by $\frac{x^2}{y^6}$, the equation becomes

$$\left(\frac{ztx}{y^3}\right)^2 = \left(\frac{x^2}{y^2}\right)^3 - a^2\left(\frac{x^2}{y^4}\right).$$

Since x and y are coprime and $y > 1$, the point $P = \left(\frac{x^2}{y^2}, \frac{ztx}{y^3} \right)$ is a point of infinite order on (11). Hence the Mordell-Weil rank of (11) is greater than 0.

Conversely, let $P = (x, y)$ be a point of infinite order on E. Let $x = \frac{s}{t^2}$ and $y = \frac{u}{t^3}$ with the GCD (s,t) = GCD(u,t) = 1. So

$$\left(\frac{u}{t^3} \right)^2 = \left(\frac{s}{t^2} \right)^3 - a^2 \left(\frac{s}{t^2} \right),$$

which produces

$$u^2 = s\left(s + at^2\right)\left(s - at^2\right)$$

after multiplying by t^6. Since GCD (s,t) = GCD(u,t) = 1, then $s, s + at^2, s - at^2$ are all mutually coprime. Thus, each is a perfect square. Letting $s = v^2$, it can be concluded that

$$v^2 + at^2 = m^2, \quad v^2 - at^2 = n^2,$$

which is a solution to (7).

It has been shown that each square-free congruent number generates a triangle with area a, as well as an elliptic curve with infinitely many rational points. Each of the rational points on the elliptic curve can be used to obtain the legs of a rational right

triangle with area a. Therefore, for each congruent number a, there are infinitely many dissimilar rational right triangles of area a [**4**].

Chapter 6: Fermat's Last Theorem and Consequences—a Conclusion

Fermat's Last Theorem was an unsolved problem in the world of number theory for close to 400 years, until Wiles used elliptic curves to finally prove Fermat's theorem. First, some work from Frey was needed [**3**, p. 170]. Frey constructed an elliptic curve based on the assumption that $a^n + b^n = c^n$ with $n > 2$:

$$y^2 = x(x - a^n)(x - b^n) = g(x). \tag{12}$$

Frey then finds the discriminant of $g(x)$, $\Delta(g) = (abc)^{2n}$. Finally, Frey postulated that an elliptic curve with such a discriminant cannot be modular.

Then, Wiles stepped in to take this idea further. Wiles investigated a large class of elliptic curves that are always modular and the proceeded to prove that (12) is always a member of that class of curves, thus providing a contradiction [**3**, p. 170].

Since the proof of Fermat's Last Theorem, elliptic curves have been used in cryptography to generate prime numbers and test numbers for primality. Atkin and Morain [**1**], for example, describe how Fermat's Last Theorem led to the Elliptic Curve Primality Proving algorithm, as well as the implementation of the algorithm. Prime numbers are used greatly in cryptography, which is discussed by Lenstra [**6**]. A problem from the 17th century is now used to further technology and electronic security.

In searching for a solution to one of mathematics' oldest questions, Fermat's Last Theorem, mathematicians have developed some very interesting and useful number

theory. Fermat's influence has reached from his time in the 1600's all the way into modern time and the future. By using elliptic curves, one can find congruent numbers, prime numbers, as well as rational right triangle areas. These advancements have allowed mathematicians to solve intriguing problems from the past. Elliptic curves may very well prove to solve other important potential problems in the years to come.

References

1. A. O. L. Atkin and F. Morain, Elliptic Curves and Primality Proving, *Mathematics of Computation*, **61** (1993) 29-68.

2. Ezra Brown, Magic Squares, Finite Planes, and Points of Inflection on Elliptic Curves, *The College Mathematics Journal*, **32** (2001) 260-267.

3. Ezra Brown, Three Fermat Trails to Elliptic Curves, *The College Mathematics Journal*, **31** (2000) 162-172.

4. Jasbir S. Chahal, Congruent Numbers and Elliptic Curves, *The American Mathematical Monthly*, **113** (2006) 308-317.

5. Charles Jepsen and Roc Yang, Making Squares from Pythagorean Triangles, *The College Mathematics Journal*, **29** (1998) 284-288.

6. H. W. Lenstra, Jr., Factoring Integers with Elliptic Curves, *The Annals of Mathematics*, **126** (1987) 649-673.

7. John Stillwell, Elliptic Curves, *The American Mathematical Monthly*, **102** (1995) 831-837.

Vita

Crystal Jensen earned her BS in Mathematics at The University of Texas at Austin, USA. She taught in Manor at Manor High School for a year, and has taught since at Georgetown High School. She is especially interested in English Language Learner teaching strategies and implementation. She currently teaches Honors Algebra II, SIOP Geometry and PreCalculus at Georgetown High School in Georgetown, Texas.

Email Address: crystal.jensen@gmail.com

This report was typed by the author.