CURVES: THE HISTORY AND DEVELOPMENT OF THE SOLUTIONS AND APPLICATIONS OF HIGHER-ORDER POLYNOMIALS

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTERS OF SCIENCE

IN THE GRADUATE SCHOOL OF THE

TEXAS WOMAN'S UNIVERSITY

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCES

COLLEGE OF ARTS AND SCIENCES

BY

DANA BLACKBURN, B.A.

DENTON, TEXAS

DECEMBER 2014

DEDICATION

This paper is dedicated to my husband Danny, for your love and support while I pursued my dreams; and to Mom and Dad, for being my foundation and my inspiration. Thank you for your never-ending love.

ACKNOWLEDGEMENTS

I would like to express my most sincere gratitude to the people who helped me achieve my dream. To my major professor, Dr. Junalyn Navarra-Madsen, I extend a heart-felt thank you for your patience, guidance, and hospitality. Your instruction in mathematics as well as your advice and counsel during my academic journey were indispensable. I could not have wanted for a better mentor.

I would like to thank Dr. Don Edwards, Chair of TWU Mathematics and member of my committee, on whom I called numerous times. Your patient responses to my frequent questioning were greatly appreciated. I am also grateful to Dr. David Marshall, for your willingness to serve as a member of my committee. I would like to say thank you to the TWU Graduate School staff for your help in formatting my thesis and meeting my deadlines.

I want to say thank you to all of my former professors, teachers, and colleagues, without whose help my journey would have been impossible. To Kendra Pearson-Scarberry, my colleague and classmate, your friendship and support helped make my dream a reality; I couldn’t have done it without you. To Mekonnen Woldehana, on whom I called so many times for help, I extend a deeply sincere thank you.

I want to acknowledge the inspiration I found in the life and works of Dr. Stephen Hawking, whom I had the great honor of meeting in November 1998. You are living proof that, no matter how great the obstacle, through strength and perseverance your dreams can become reality.

To my family I extend my deepest gratitude; without your help and support this would not have been possible. I want to say thank you to my husband Daniel, for taking care of everything at home while I focused on my graduate work. I appreciate you for all you have done so that I could realize my dream. Thank you for your love, generosity, and support. I love you, honey.

To my mother and father, I want to extend an especially warm, heart-felt thank you.   For all the years you’ve taken care of me, inspired me, consoled me, lifted me up, and cheered me on, words cannot express the deepness of the gratitude I feel. I love you both and thank you so very much for everything you have done for me.

And finally, I want to say thank you to my Heavenly Father and my Lord and Savior, Jesus Christ. To Him goes all the glory, and in Him all things are possible, as I am living proof.

Figure 1. *Dana Blackburn with Stephen Hawking, November 1998*.

ABSTRACT

DANA BLACKBURN

CURVES: THE HISTORY AND DEVELOPMENT OF SOLUTIONS AND APPLICATIONS OF HIGHER-ORDER POLYNOMIALS

DECEMBER 2014

The purpose of this thesis is to explore algebraic curves, from definition and origination to development and technological / scientific application.

A broad and oft-underappreciated topic, I will begin by exploring algebraic curves based on their degrees. Each chapter of my paper will be dedicated to an algebraic degree, beginning with 1st degree and concluding with 5th degree polynomials. In each chapter, we will look at the history and timeline of mathematical methods associated with that particular degree, along with a biography of major players in its discovery and subsequent achievements.

The treatment of each degree will finalize with a look at technological and scientific achievements that can be, at least in part, attributed to the mathematics behind it. We will even observe that the rate of change of our technological growth almost seems to model the numeric growth of our topic; i.e., what began as a slow, almost constant rate of change (degree 1) with ancient societies has accelerated through the centuries (and indeed, millennia) to an exponential rate (degree 3). My work will

conclude with a look at what potentially lies before us if our technology continues to grow at this rate.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER I

THE DEGREE OF A CURVE

Introduction

The following overview was heavily inspired by the work entitled, “Elliptic Tales: Curves, Counting, and Number Theory”, Avner Ash and Robert Gross.

Curves can be defined by their degree, and algebraic curves can be defined by the degree of their polynomial equations. The degree of a curve (and that of its generating polynomial) is a useful tool in arranging and describing algebraic and geometric objects. These objects can be arranged by their respective degrees into a natural hierarchical order from the simple to the complex.

The concept of a curve has been long studied by various ancient civilizations, arguably most successfully by the ancient Greeks. They mastered construction techniques involving lines, planes, and circles, using primarily a straightedge and a compass. These tools, of course, limited them to curves of degrees 1 and 2.

Greek mathematics did advance to the point of constructing higher degree and non-algebraic curves, such as spirals. These techniques took them beyond what could be done with the straightedge and compass; instead, they discovered methods that included doubling the cube and trisecting angles (both of which are problems of degree 3).

Doubling the cube involves solving the equation $x^3 = 2$, clearly a problem of degree 3. Angle trisection involves finding the intersection of a circle and hyperbola, which can be written as an equation of degree 3.

The complexity of curves advances with the level of their respective degrees; e.g., a curve of degree 1 (a line) is less mathematically complex than a curve of degree 2 (a circle), which in turn, is less complex than a curve of degree 3 (a cubic). Delving deeper into the latter, a cubic curve can be compared graphically to a sine wave. However, differences in their properties give each of them distinct characteristics. An algebraic curve of degree 3 has exactly 3 roots; that is, there are 3 real or complex independent values (counting multiplicity) which produce a dependent value equal to zero. A sine wave, however, has no limit to its number of roots. It does, however, have an upper and lower limit to its range, along with an unbounded domain.

This provides a nice segue to define the degree of a curve. As mentioned earlier, an algebraic curve of degree 3 has exactly 3 roots. These roots can be described as the intersections of the algebraic curve with the line $y = 0$ (a.k.a., the x-axis). This line of intersection is called a “probing line”, a line which reveals the geometric degree. Therefore, we can now define the *geometric degree of a curve* to be the *maximum number* of these intersection points.

The aforementioned curves are described graphically in 2-dimensional space; however, introducing an additional variable can extend our study into objects of 3-space. Consider the following equation:

$$x^2 + y^2 + z^2 = r^2$$

The introduction of the z^2 term transforms a 2-dimensional circle into a 3-dimensional sphere, all in one stroke! So how do we graph this sphere? Mathematically, we first define the solution set to be the set of all triples of the form:

$$(x, y, z) = (a, b, \pm\sqrt{r^2 - a^2 - b^2})$$

To get a single solution, simply pick any two numbers for *a* and *b*, and let those be the values of *x* and *y*. Then, substitute these into the equation to produce the value of *z*.

While single equations are sufficient to describe a curve in 2- or 3-dimensional space, considering curves in higher dimensions becomes easier if we first parameterize the equations. A parameter is simply an extra variable, often represented by *t*. A system of equations in parametric form is one in which the original variables are set equal to functions of the parameters. Therefore, to describe a curve in the *xy*-plane, we could use the *t*-parameter in function notation to write x = f(t) and y = g(t).

The concept of parametric equations can be clarified through a simple example. Consider the slope-intercept form of a linear equation: y = mx + b. This form is perfectly fine in describing most linear equations, with one exception: the vertical line. Since this line has an undefined slope, it cannot be expressed in this form. The equation of this line is of course x = *c*, where *c* is some constant. However, if we *parameterize* this line, it can be easily expressed algebraically in terms of *x* and *y*. Here's how: let *a, b, c,* and *e* be any real numbers. Then in the *xy*-plane, the equation of the vertical line in the form x = e can be written as:

$$x = e$$
$$y = t$$

In fact, assuming a non-zero *a* or *c*, any line can be parameterized in this form:

$$x = at + b$$
$$y = ct + e$$

Another way to think about a parameter is to imagine a line or curve being described by a moving point. At any moment in time *t*, the curve is at location *P(t)*. We can write the coordinates of $P(t) = (x(t), y(t))$. A good analogy here is to visualize the moving point as a planet revolving around the sun. Then, the set of all possible points occupied by the moving point is its "orbit". This example will lead us into the concept of spheric equations of degree 3, which we will explore in chapter 3.

Let's return to the discussion of the definition of degree. The opening paragraph stated that curves could be defined by their degree. We will see, however, that there are cases where this does not hold true, at least in the case of real numbers. For example, let G be the graph of $x^2 + y^2 + 1 = 0$. What real number solutions exist on this graph? None! Because the square roots of real numbers cannot be negative, the solution set of G is empty (it would only be defined in the set of complex numbers). This example proves that we can have a polynomial of degree 2 that describes a geometric object of degree zero.

An important observation can be made here: given a polynomial of degree “d”, any probing line will intersect it in *at most* “d” points. This agrees with our earlier definition: the geometric degree of a curve can be described as the *maximum number* of these intersection points.

Now, let’s take a closer look at curves by exploring each one by its degree.

CHAPTER II

CURVES: 1ST AND 2ND DEGREE -- LINEAR AND QUADRATIC

History and Development of Solutions

The concept of a curve has been long studied by various ancient civilizations. The search for curves' solutions and their resulting significance has been a focus of mathematicians and philosophers alike, dating from time immemorial.

Often Babylonians of about 400 BC are credited to be the first to solve quadratic equations. They developed an algorithmic approach that led to the quadratic equation and essentially solved by completing the square (O'Connor & Robertson, 1996). However, work on the mathematical properties of line and closed figures (degrees 1 and 2) had been done much earlier.

While many civilizations developed sophisticated mathematical techniques in this field, advancements in this area were done arguably most successfully by the ancient Greeks. They mastered construction techniques involving lines, planes, and circles, using primarily a straightedge and a compass. These tools, of course, limited them to curves of degrees 1 and 2. The ancient Greeks were masters of solving and utilizing curves of degrees 1 and 2; in fact, Euclid's geometrical approach to finding length is the method currently used to find the root of a quadratic equation (O'Connor & Robertson, 1996). In addition to Euclid (300 b.c.) other great mathematicians from the Greek culture include Thales (600 b.c.), Pythagoras (550 b.c.), Archimedes (250 b.c.), Eratosthenes (230 b.c.), Ptolemy (150 a.d.) and Diophantus (250 a.d.) (Davis, 1993).

Pythagoras of Samos is credited with the famous theorem

$$a^2 + b^2 = c^2$$

which relates the hypotenuse length *c* of a right triangle to the lengths *a, b* of the other sides. Pythagoras' famous theorem has certainly earned universal notoriety and accolades for its elegant and far-reaching applications, and the background of Pythagoras himself is as interesting as his famous theorem. An image of Pythagoras can be seen in Figure 2.

Early on in his life, Pythagoras is thought to have travelled to Egypt and Mesopotamia, acquiring scientific and mathematical knowledge. Later, he founded a secretive society called the "Pythagorean School" in Crotone, on the southern coast of modern Italy – part of Magna Graecia in the time a Pythagoras. The followers of Pythagoras supposedly shunned individuality, and believed that the discovery and stewardship of knowledge should be a communal endeavor: it was their custom to credit all discoveries to their leader. It is believed that the Pythagorean school was ultimately destroyed in a political upheaval. Pythagoras himself fled Crotone, but was pursued and killed in Metapontum (Farouki, 2008).

Figure 2. *Pythagoras*

As of yet, no written document from the Pythagoreans has ever been found; what we know of their ideas and accomplishments came from others. However, historical research tells us they were most likely the first intellectual society. Members of the Pythagorean School pursued mathematics and philosophy simply for the benefit of society and its moral advancement. Pythagoras himself supposedly coined the terms *philosophy* for “love of wisdom”, and *mathematics* for “that which is learned” to describe the goals of his school. Their motto, “*all is number*”, expresses their faith in the unity of nature’s latent mathematical structure, with its diverse manifestations in musical harmony, the planetary motions, and other natural phenomena (Farouki, 2008).

As an interesting side note, in medieval times, the *quadrivium*, or “four paths” (arithmetic, geometry, music and astronomy) complemented the *trivium*, or “three paths” (grammar, dialectic, and rhetoric) to form the *seven liberal arts*. These four studies compose the secondary part of the curriculum outlined by Plato in *The Republic*, and are described in the seventh book of that work. The quadrivium is implicit in early Pythagorean writings . As Proclus wrote:

"The Pythagoreans considered all mathematical science to be divided into four parts: one half they marked off as concerned with quantity, the other half with magnitude; and each of these they posited as twofold. A quantity can be considered in regard to its character by itself or in its relation to another quantity, magnitudes as either stationary or in motion. Arithmetic, then, studies quantities as such, music the relations between quantities, geometry magnitude at rest, spherics [astronomy] magnitude inherently moving" (www.princeton.edu).

In other words, arithmetic was the study of *pure number*, with geometry of *number in space*, music of *number in time*, and astronomy as *number in space and time* (Farouki, 2008).

After discovery of the inherent properties of all right (90 degree) triangles, and hence creation of the Theorem, the Pythagoreans became interested in finding examples of natural numbers that satisfied its conditions. Certainly they were familiar with the simplest triple (3, 4, 5) employed by the Egyptians in the construction of the pyramids. However, they took their research a step further and developed a procedure to *construct* such triples, by inserting odd numbers *m* in the expressions

$$a = \frac{1}{2}(m^2 - 1), \qquad b = m, \qquad c = \frac{1}{2}(m^2 + 1).$$

This was subsequently generalized in Euclid's Elements, where it is shown that, for integers *u* and *v*, the formulae

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2$$

yield all Pythagorean triples (Farouki, 2008).

What makes the Pythagorean Theorem so integral and applicable, as well as timeless, is that it lies at the foundation of *distance measurement,* given by the formula

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

between two points (x_1,y_1) and (x_2,y_2). Later, with the advent of calculus, it became possible to precisely define not only a straight-line distance between two points, but also the distance along a curved path, i.e., to *rectify* (compute the arc length of) curves.

Per Farouki in "*Pythagorean-Hodograph Curves*", applying the Pythagorean theorem to an infinitesimal segment dε of a differentiable parametric curve r(ε) = (x(ε), y(ε)) allows us to express its arc length as

$$ds = \sqrt{x'^2(\varepsilon) + y'^2(\varepsilon)}\ d\varepsilon$$

and the total arch length S of a finite segment $\varepsilon \in [a, b]$ is thus given by the integral

$$S = \int_a^b \sqrt{x'^2(\varepsilon) + y'^2(\varepsilon)}\, d\varepsilon.$$

To obtain a closed-form reduction of the integral (thereby making it computable), the integrand must admit an indefinite integral – or "anti-derivative" – expressible in terms of known analytic functions, i.e., we must be able to identify a function s(ε) such that

$$\frac{d}{d\varepsilon}\,\mathrm{s}(\varepsilon) = \sqrt{x'^2(\varepsilon\,) +\; y'^2(\varepsilon\,)} \quad \text{(Farouki, 2008).}$$

Greeks preferred to conduct mathematical work in purely geometrical terms. For example, Archimedes set about to calculate an area enclosed by a curve, such as a circle. He achieved this using a method called "exhaustion" (Davis, 1993), which approximates the whole area using sums of area of triangles. This works by letting the triangles "exhaust" the region by finer and finer approximations (Davis, 1993). He developed a similar method for calculating volumes. His method of exhaustion essentially became integral calculus, nineteen hundred years later (Davis, 1993).

Around the last third of the 5th century B.C., Greek mathematics advanced to degrees 3 and beyond (Dieudonne, 1985). These techniques took them beyond what could be done with the straightedge and compass; instead, they discovered methods that included doubling the cube and trisecting angles (both of which are problems of degree 3, and will be discussed in a later chapter).

The Importance of the Quadratic Discriminant

Given a quadratic function in the general form f(x) = ax^2 + bx + c, one can easily find the roots of the function (points of intersection with the x-axis) by applying the quadratic formula. This formula is derived from the general form of a quadratic by completing the square (Table 2).

Table 1.

Deriving the Quadratic Formula.

Start with the general form quadratic, set equal to zero.	$ax^2 + bx + c = 0$
Set equation equal to the constant *c*, and divide by *a*.	$x^2 + \frac{bx}{a} = -\frac{c}{a}$
Complete the square by adding $[(\frac{1}{2})(\frac{b}{c})]^2$ to both sides.	$x^2 + \frac{bx}{a} + \frac{b^2}{4a^2} = -\frac{c}{a} + \frac{b^2}{4a^2}$
Rewrite the perfect square trinomial as a binomial squared. Rewrite right-side terms with common denominator.	$(x + \frac{b}{2a})^2 = -\frac{4ac}{4a^2} + \frac{b^2}{4a^2}$
Take the square root of both sides.	$\sqrt{(x + \frac{b}{2a})^2} = \pm\sqrt{\frac{b^2 - 4ac}{4a^2}}$
Simplify.	$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$
Subtract $\frac{b}{2a}$ from both sides.	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Deriving the quadratic formula reveals one of its most useful features – the *discriminant*. The discriminant is the radicand of the quadratic formula, $b^2 - 4ac$, and is denoted by Δ.

Arguably the most useful function of the discriminant is its ability to reveal the *number* of real roots of a quadratic equation. It is called the discriminant because, using its value, one can *discriminate* (tell the differences) between the various solution types. The characteristics of the discriminant are outlined in Theorem 1, the proof of which can be easily found in a number of elementary algebra textbooks.

Theorem 1: Quadratic Discriminant. Evaluating the quadratic discriminant $b^2 - 4ac$ with the real coefficients of the quadratic will result in one of three outcomes:

i. If $b^2 - 4ac > 0$, we can take the square root of this positive amount, and the result will be two unique, real roots (multiplicity 1)

ii. If $b^2 - 4ac = 0$, we will be adding and subtracting zero, meaning there is only one real root (multiplicity 2).

iii. If $b^2 - 4ac < 0$, the square root will be of a negative number, which is not defined over the set of real numbers. However, the roots do exist as a complex conjugate.

The proof of this theorem can be found in a number of elementary algebra textbooks.

Applications

Linear functions – those of degree 1 – form the basis of quadratics, and quadratic functions – those of degree 2 – are the foundation of many objects and technologies that have changed our lives. The inherent properties of the parabola – the shape formed from graphing quadratic functions - lend themselves to a wide variety of applications. These applications extend from the mundane, such as headlights and snow skis, to the highly technical, such as satellite dishes that allow global communications and seemingly instant data transfer. Applications of quadratics even extend into cosmology; one of Einstein's equations, the metric form of a quadratic, is used to model the structure of spacetime (superstringtheory.com).

Parabolic Skis

Let's begin our discussion on the applications of quadratics with a recreational object enjoyed by many – the snow ski. In the last decade of the 20th century, our basic snow ski began to take on a new shape. Traditional straight-edged skis were being supplanted by those with a sleeker, curvier design – one that was wider at the ends and narrower in the middle. Enthusiasts began to wonder, was this new design simply esthetic, created solely as a marketing ploy? Or, was there real value to be gained from a redefined shape?

The answer was the latter: these new skis with their parabolic shape greatly outperformed their straight-edged predecessors. The straight-edged skis had to be maneuvered by putting enough force on the ski to create an arc. This force had to be used along with rotation in order to "set" the edge of the ski and carve a turn. Needless to say, the level of physical strength and stamina required to maneuver these skis excluded many children and older adults from taking part in the sport (www.parabolicskis.com).

The parabolic shape – wide at the ends and narrow in the "waist" of the ski – is created with what is called a "sidecut" (Figure 3). This sidecut allows the skier to turn by simply shifting his or her weight toward the edge of the ski; the weight then engaged the sidecut, which would carry the ski through the turn (www.parabolicskis.com).

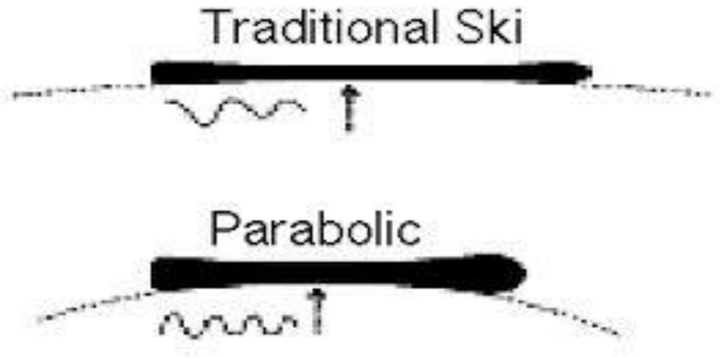


Figure 3. *Traditional vs. Parabolic Skis*. Courtesy of www.parabolicskis.com.

The result of this parabolic sidecut was a quicker response to minimal pressure by the skier, allowing for easier turns and a more fluid ride.

Satellite Dishes

Many young people today cannot imagine a world in which wireless communication doesn’t exist. These children’s lives revolve around the use of their wireless device. Ask any parent or school teacher and most will agree that the majority of kids are so attached to their wireless devices, they would rather make any sacrifice necessary (lose grades, lose privileges, accept alternate punishment, etc.) in order to keep it with them at all times (and as a former public high school teacher, I can attest to this firsthand). However, most of these young people aren’t aware that the very existence of this technology is made possible by the simple parabola.

How is a parabola responsible for technology which has become so entrenched in our collective lives? The answer – it is the basis of the satellite dish. Satellite dishes are the terrestrial tools which allow signals to be sent to and received from satellites; this in turn allows for seemingly instant communication. A parabola enables the dish to accomplish this due to one of its most fundamental – and beautiful – properties. At a specific point above the parabola – a point called the "focus" – every single line that enters the parabola parallel to its axis will be reflected to intersect at that precise point – regardless where within the parabola the line hits. Here is how it works.

The parabola is made up of points which are all equidistant from a fixed point, the "focus", and a fixed line, the "directrix". Construct a curve on a coordinate plane such that the focus is the point F (0,p) and the directrix is the horizontal line y = -p. Any given point (x,y) will only be on the line if the distance from (x,y) to the focus is equal to the distance from (x,y) to the directrix (Weston, 1995). Equating the squares of these distances (to avoid dealing with square roots), we get the equation:

$$(x – 0)^2 + (y – p)^2 = (y + p)^2.$$

Expanding and simplifying gives us:

$$y = \frac{x^2}{4p}$$

as the equation of the parabola (Weston, 1995).

Imagine there is a satellite directly above us, so we tilt our parabolic dish to point at it. The satellite is far enough away that we can assume all of the signals are coming in vertically, parallel to the dish's axis. Suppose that a particular signal strikes the dish at the point P with x-coordinate a. Therefore, the coordinate of P is $\left(\text{a}, \frac{a^2}{4p}\right)$ (Weston, 1995). Extend a vertical line through P to meet the directrix at a point Q (a, -p). The midpoint S of the line segment FQ has coordinates $\left(\frac{a}{2}, 0\right)$, clearly residing on the x-axis (Figure 4)(Weston, 1995).

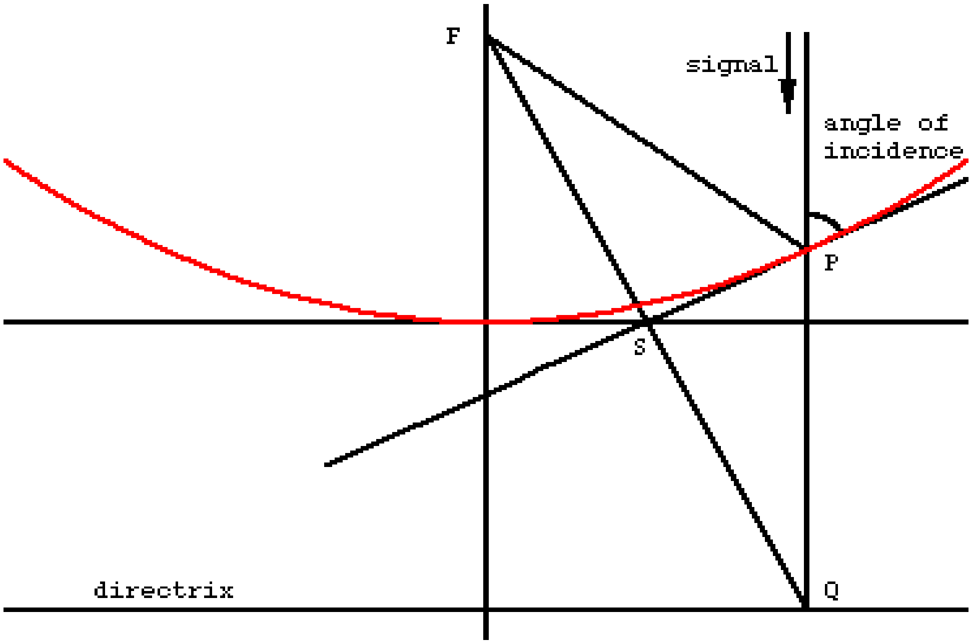


Figure 4. *Focus and Directrix of a Parabolic Satellite Dish*. Courtesy of www.parabolicskis.com.

A line tangent to the parabola at point P will intersect the x-axis a point S, the midpoint of FQ. Since $|FP| = |PQ|$, triangles FPS and QPS are congruent; therefore, angles FPS and QPS are equal. Angle QPS and the angle of incidence are vertical angles, meaning they are also equal. The vertical signal travelling along the line PQ will, therefore, reflect off the dish at point P and pass directly through the focus F (Weston, 1995). This will be the same for all vertical signals that hit the satellite dish: regardless of location on the dish, every signal that strikes it will reflect and pass through the focus. Thus, the satellite manufacturer will position the receiver at that focal point to pick up those signals, and communication has been established.

CHAPTER III

CURVES: 3rd DEGREE – THE CUBIC

Introduction

The discovery of solutions to cubic equations (and indeed, any equation of degree ≥ 3) marked a major jump in the advancement of mathematics, for several reasons. Firstly, it was the most notable advancement since the time of the ancient Greeks. Secondly, it was the first mathematical formula *unknown* to the ancients. Thirdly, and most importantly, it led to the study of the theory of equations, culminating in the nineteenth century in the proof of the insolvability of the quintic (Villanueva, 2013). The latter will be discussed in the conclusion of this paper.

An elliptic curve is considered the simplest curve after lines and conics (Verrill, 2004). While their name implies a relationship to ellipses (a type of conic), there all semblances end; their form is much more complex. That being said, the elliptic curve can be handled and understood much more easily than a quartic (or higher order polynomial); this is in part due to a unique characteristic of this curve: the elliptic can be viewed as a group.

Graphically, the solutions to an elliptic curve lie on a torus - a surface the shape of a doughnut. The particular type of curve is given by the Weierstrass form of the equation

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

where the discriminant is nonzero (Silverman, 2006).

Theorem 2: Cubic Discriminant. Given the Weierstrass equation $y^2 = x^3 + ax + b$, the discriminant derived will be of the form

$$\Delta = 4a^3 + 27b^2$$

Given the function $f(t) = t^3 + pt + q$. If $p \geq 0$, the function is continually increasing so it has only one real root. In this case, the following inequality is true: $Let\ \Delta => 0$. However, if $p < 0$, then the function has two critical values (one maximum and one minimum), found by setting $f'(t) = 0$ at $t = \pm\sqrt{\frac{-p}{3}}$. The function has three real roots if and only if the y − coordinates of these points have opposite signs; meaning, if and only if

$$F\left(\sqrt{\frac{-p}{3}}\right) F\left(-\sqrt{\frac{-p}{3}}\right) < 0$$

This corresponds directly to $\frac{q^2}{4} + \frac{p^2}{27} < 0$.

In summary, given $\Delta = 4a^3 + 27b^2$; this is called the discriminant of the cubic.

- If $\Delta > 0$, then there exists only one real root.

- If $\Delta < 0$, then there exist three real roots.

- If $\Delta = 0$, the equation can have one or two real roots (if it has two real roots, one of them is repeated. You can find the repeated root by setting the derivative equal to zero and using the quadratic formula or factoring if able (McClendon, 2011).

If we define our cubic curve over a field K, such that the product of K × K is a plane over the field K, with the set of points (x,y) forming a subset of the plane, the curve can then be more accurately described as

$$C = \{(x,y) : y^2 = x^3 + ax + b\} \subset K^2 \}$$

The basic equation can be rewritten as a product of linear factors in the form:

$$C = x^3 + ax + b = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3),\ \lambda_i$$

where λ_i is an element of K for all *i*.

The resulting roots reveal characteristics of the function as such:

i. C is a *smooth* curve, if the three roots λ_i are all unique.

ii. C is a *nodal* curve, if two of the λ_i coincide (multiplicity two) and one is unique.

iii. C is *cuspidal* curve, if the three roots λ_i are all identical (Szendroi, 2005).

A cubic curve can be derived from an ellipse if we take the integral of its arc length and parameterize it with a change in variables. Taking the integral of a standard ellipse $\frac{s^2}{a^2} + \frac{t^2}{b^2} = 1$ gives us its arc length from the point (0,b) to some point (s, t), as such:

$$\int_0^s \left(\frac{1 - e^2 u^2}{1 - u^2} \right)^{½} \text{(Szendroi, 2005)}$$

Where $u = \frac{s}{a}$, and $e^2 = 1 - \frac{b^2}{a^2}$. If we let *v* represent the integrand, then the following quartic equation holds true and expresses the relationship between variables.

$$u^2v^2 - e^2u^2 - v^2 + 1 = 0$$

This quartic can then be transformed into a cubic equation by introducing a new set of variables (x, y) as an invertible rational map, which then can be algebraically transformed into the standard cubic equation (Szendroi, 2005).

If e = 0, the ellipse is transformed into a nodal cubic curve. However, if $e \neq 0$, then the ellipse is transformed into a smooth cubic curve. Integrals of this type are called *elliptic integrals*, and the resulting cubic curve called an *elliptic curve.*

One of the defining characteristics of smooth elliptic curves is their adherence to abelian group law. This characteristic exists due to the smooth elliptic curve's construction, and the fact that its degree is precisely three.   Take two points P = (x_p, y_p) and Q = (x_q, y_q) on an elliptic curve C, such that

$$C = \{(x,y) \in \mathbb{R} : y^2 = x^3 + ax + b\}$$

Connecting the points with line PQ creates a linear equation in the form *y = mz + n.* Substituting this line into the above cubic equation will create a cubic equation for the x-coordinates of the intersecting points (Szendroi, 2005). Two of these coordinates are x_p and x_q; therefore, a third intersection point must exist, which we will call R (x_r, y_r). Allowing for special cases (such as when P = Q, in which case R = ∞ will be the extra point), the assertion can be made that for every pair of points P, Q on C ∪ {∞} with an existing third point R.   As a result, all pairs of points P, Q adhere to the group law's properties of associativity, commutativity, invertibility, and laws of identity.

History and Development of Solutions

Solutions to cubics in the form of curves can be traced back through the millennia. Notable people in this area of achievement include Omar Khayyam (1048-1123), who used intersections of conics to give the geometric constructions of cubic roots, as well as Leonardo de Pisa (Fibonacci) (1180-1245), who developed an approximation formula for certain forms of the cubic (Villanueva, 2013).

The Babylonians were able to evaluate cubic expressions; in fact, Babylonian mathematics went far beyond just arithmetical calculations. The Babylonians were famed as constructors of tables, which could be used to solve equations. For example, they constructed tables for the expression $n^3 + n^2$; hence, with the aid of these tables, certain cubic equations could be solved (figure 5).

For example, consider the equation

$$ax^3 + bx^2 = c.$$

Figure 5: *Babylonian Cuneiform Tablet*.

Our notation here is modern, and completely different from the position-specific cuneiform they used (see Figure 5). However, the Babylonians were able to solve numeric equations as such, using established rules along with numeric tables. In our example, they would multiply the equation by a^2 and divide it by b^3 to get

$$(ax/b)^3 + (ax/b)^2 = ca^2/b^3.$$

Putting $y = ax/b$ this gives the equation

$$y^3 + y^2 = \frac{ca^2}{b^3}$$

which could now be solved by looking up the $n^3 + n^2$ table for the value of n satisfying $n^3 + n^2 = \frac{ca^2}{b^3}$. When a solution was found for y, then x was found by $x = \frac{by}{a}$. It is important to note that all this was done without algebraic notation and showed a remarkable depth of understanding.

However, the discovery of solutions to cubic *equations* first occurred in the sixteenth century in Italy, by Scipione del Ferro (1465-1526), a lecturer in arithmetic and geometry at the University of Bologna from 1496 until 1526. He was the first to discover the solution to the cubic, which he wrote in a manuscript (unfortunately the manuscript did not survive over time; in fact, no manuscripts by del Ferro are known to survive to this day). The problem was to find the roots by adding, subtracting, multiplying, dividing and taking roots of expressions in the coefficients. It is believed that del Ferro could only solve cubic equation of the form $x^3 + mx = n$; without knowledge of negative numbers, his solution could not be used to solve all cubics (O'Connor & Robertson, 1996). At that time, the general solution to the cubic still awaited discovery.

Later, on his deathbed, del Ferro passed the manuscript to one of his students, Antonio Fior. Fior, now in possession of the sought-after solution, was not very good at keeping secrets. Soon news of this ground-breaking discovery spread and reached the mathematician Niccolo Tartaglia. His surname, Tartaglia, means "the stammerer"; he was dubbed this name after a sword cut to the tongue during a French siege of Brescia rendered his speech difficult (Petrov, n.d.). Tartaglia was enticed by the rumors to pursue his own solution, which he accomplished. He solved cubics in the form $x^3 + mx^2 = n$.

Like Fior, Tartaglia was not good at keeping secrets, and was vocal about his accomplishment. This prompted Fior to challenge Tartaglia to a public contest, which he accepted. The conditions of the contest were that each gave the other 30 problems with 40 or 50 days in which to solve them, the winner being the one to solve most but a small prize was also offered for each problem (O'Connor & Robertson, 1996). Tartaglia's was a convincing victory: he managed to solve all Fior's problems in the space of 2 hours! It turns out that all the problems Fior issued were of the form $x^3 + mx = n$, which he believed Tartaglia would be unable to solve. Tartaglia then took his accomplishment a step further -- only 8 days before the problems were to be collected, Tartaglia discovered the general method of solution for *all* types of cubics (O'Connor & Robertson, 1996).

Tartaglia, although verbally impeded, was not shy about proclaiming his achievement. Word of it travelled, and eventually came to the attention of Girolamo Cardano, an Italian doctor and mathematician living in Milan. Cardano wanted to learn more about this purported solution and its author, so he invited Tartaglia for a visit. During this visit, Cardano very persuasively convinced Tartaglia to share the secret of his solution of the cubic equation. While Tartaglia agreed, he stipulated one non-negotiable condition: Cardano must swear to keep the solution secret until Tartaglia had published it himself. Additionally, Tartaglia only agreed to reveal it in written form as code, elaborately worded into a poem. This way, if Cardano passed on, no one else could acquire and understand it. Tartaglia's poem read as follows:

When the cube and things together
Are equal to some discreet number,
Find two other numbers differing in this one.
Then you will keep this as a habit
That their product should always be equal
Exactly to the cube of a third of the things.
The remainder then as a general rule
Of their cube roots subtracted
Will be equal to your principal thing
In the second of these acts,
When the cube remains alone,

You will observe these other agreements:

You will at once divide the number into two parts

So that the one times the other produces clearly

The cube of the third of the things exactly.

Then of these two parts, as a habitual rule,

You will take the cube roots added together,

And this sum will be your thought.

The third of these calculations of ours

Is solved with the second if you take good care,

As in their nature they are almost matched.

These things I found, and not with sluggish steps,

In the year one thousand five hundred, four and thirty.

With foundations strong and sturdy

In the city girdled by the sea. (O'Connor & Robertson, 2005).

Applications

In the field of number theory, a problem which appears at first glance to be a simple Diophantine equation (i.e., an equation is one where the coefficients are whole numbers, and where the solution is also constrained to be a whole number), can lead into something much more complex -- an elliptic curve.

Elliptic curves have many applications in our modern day world, as well as many important areas of mathematics and its applications. These areas include topology, number theory, complex analysis, physics, and cryptography (the latter of these, cryptography, is discussed later in detail). It was work he did on elliptic curves that finally allowed Andrew Wiles to prove Fermat's Last Theorem (http://plus.maths.org).

Let’s take a look at one use of elliptic curves which has serious and important applications in modern day technology – elliptic curve cryptography.

Elliptic curves as algebraic/geometric entities have been studied extensively for the past 150 years, and one of the results of this research – elliptic curve cryptography – has had a profound impact on modern day technology. Given the prevalence of digital technology, i.e., data and communication created in digital format for almost instant access from any location on any platform, the need for data security becomes paramount. Elliptic curve cryptography provides that high level of technological security.

Many companies have entered the marketplace of data security by creating products that offer guaranteed data security; one such company is Certicom. Founded in 1985 and headquartered in Ontario, Canada, Certicom states that its encryption software “protects billions of dollars’ worth of content and millions of devices around the world. With over 350 patents and patents pending worldwide covering key aspects of Elliptic Curve Cryptography (ECC), Certicom provides the core technology for the National Security Agency (NSA) Suite B standard for secure government communications. As the world-leading expert in public key infrastructure implementations, device security, anti-counterfeiting, product authentication, asset management, and fixed-mobile convergence, many industry-leaders -- IBM, Continental Airlines, Aristocrat Technologies, Cavium, General Dynamics, Motorola, Oracle, Research In Motion (RIM), Unisys, XM, Bally Technology, General Electric, Texas Instruments, Qualcomm, Mitre, L-3, Phillips, Samsung, Sony Ericsson, and Nortel -- have become Certicom customers." (www.certicom.com/about)

Elliptic Curve Cryptography

This section discusses how companies like Certicom utilize elliptic curve cryptography to provide data security to their clients, and is based upon information gleaned from Certicom's website. The foundational logic of most cryptographic systems is based on algebraic group properties. An algebraic group is a set whose elements adhere to the following properties: associativity, commutativity, invertibility, and identity. For elliptic curve groups, these operations are defined geometrically. The field over which the elliptic curve resides is given strict properties; these properties define the field into a lattice. Generally, elliptic curves reside on underlying fields F_p (*where p is a prime*) and F_2m (*a binary representation with 2^m elements*).

Given the Weierstrass Normal Form of an elliptic equation,

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

if the discriminant Δ ≠ 0, then the elliptic curve is smooth and can be used to form a group.

Substituting different values for *a* and *b* will result in a different elliptic curve. For example, a = -4 and b = 0.67 gives the elliptic curve with equation $y^2 = x^3 - 4x + 0.67$; the graph of this curve is shown below (Figure 6).

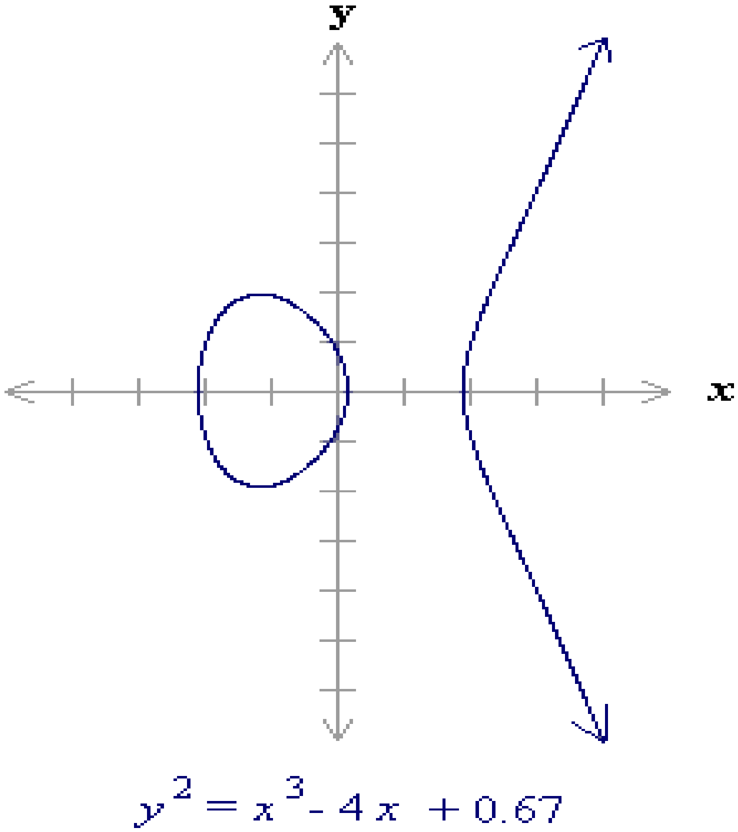


Figure 6. *Elliptic Curve.*

Elliptic curve groups are additive groups; that is, their basic function is addition. The addition of two points in an elliptic curve is defined geometrically. The negative of a point P = (x_p,y_p) is its reflection in the x-axis: the point -P is $(x_p,-y_p)$. Notice that for each point P on an elliptic curve, the point -P is also on the curve (www.certicom.com).

Suppose that P and Q are two distinct points on an elliptic curve, and the P is not -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R. For example:

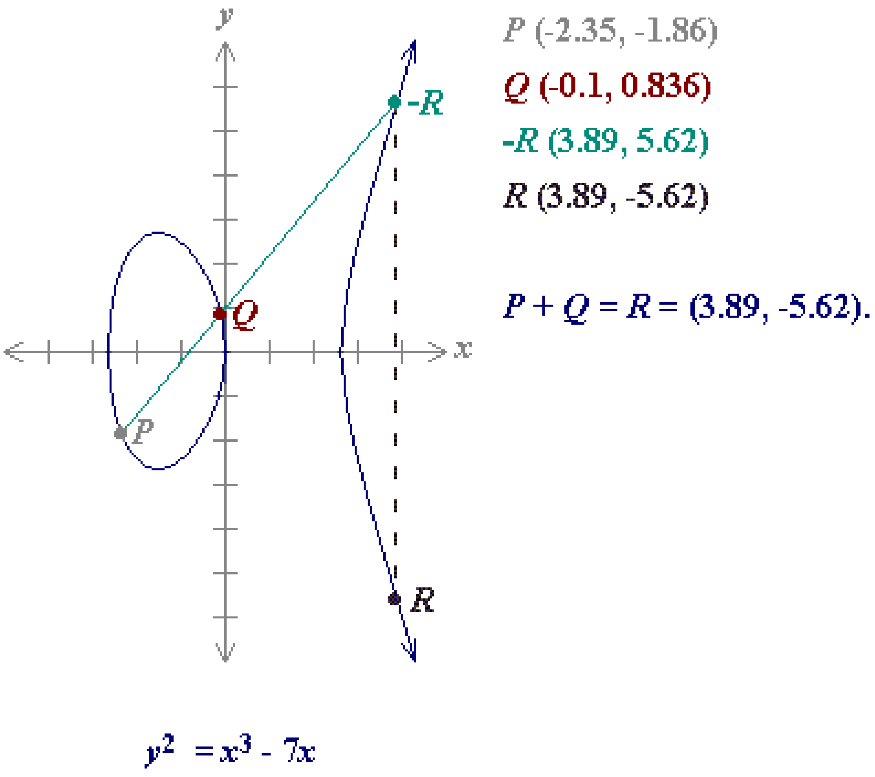


Figure 7. *Adding Distinct Points P and Q*

The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and -P cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity 0. By definition, P + (-P) = 0. As a result of this equation, P + 0 = P in the elliptic curve group . 0 is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity.

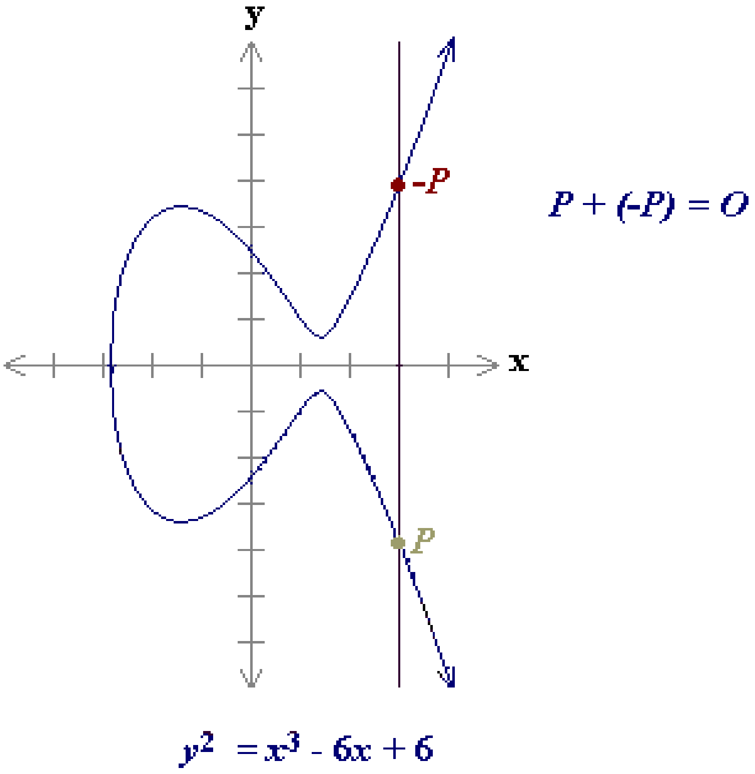


Figure 8. *Adding the Points P and -P*

To add a point P to itself, a tangent line to the curve is drawn at the point P. If y_P is not 0, then the tangent line intersects the elliptic curve at exactly one other point, -R. -R is reflected in the x-axis to R. This operation is called doubling the point P; the law for doubling a point on an elliptic curve group is defined by P + P = 2P = R.

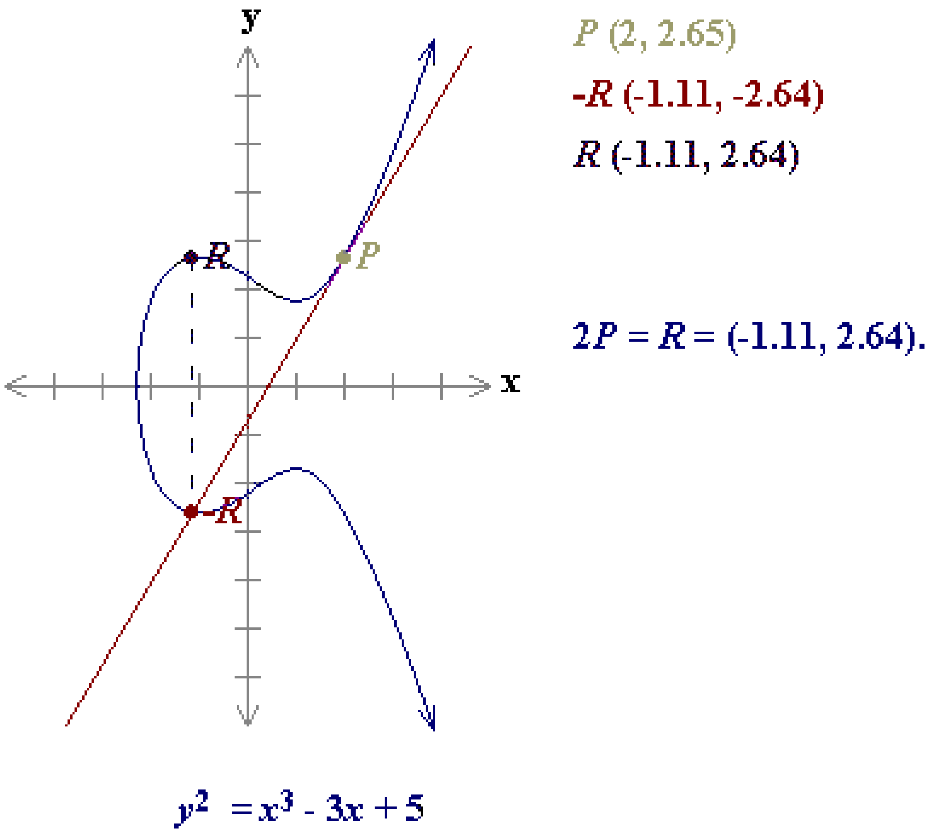


Figure 9. *Doubling the Point P: multiplicity 2*

The tangent from P is always vertical if $\mathbf{y}_P = 0$. If a point P is such that $\mathbf{y}_P = 0$, then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point. By definition, 2P = 0 for such a point P. If one wanted to find

3P in this situation, one can add 2P + P. This becomes P + 0 = P Thus 3P = P.

3P = P, 4P = 0, 5P = P, 6P = 0, 7P = P, etc.

Although the previous geometric descriptions of elliptic curves provides an excellent method of illustrating elliptic curve arithmetic, it is not a practical way to implement arithmetic computations. Algebraic formulae are constructed to efficiently compute the geometric arithmetic.

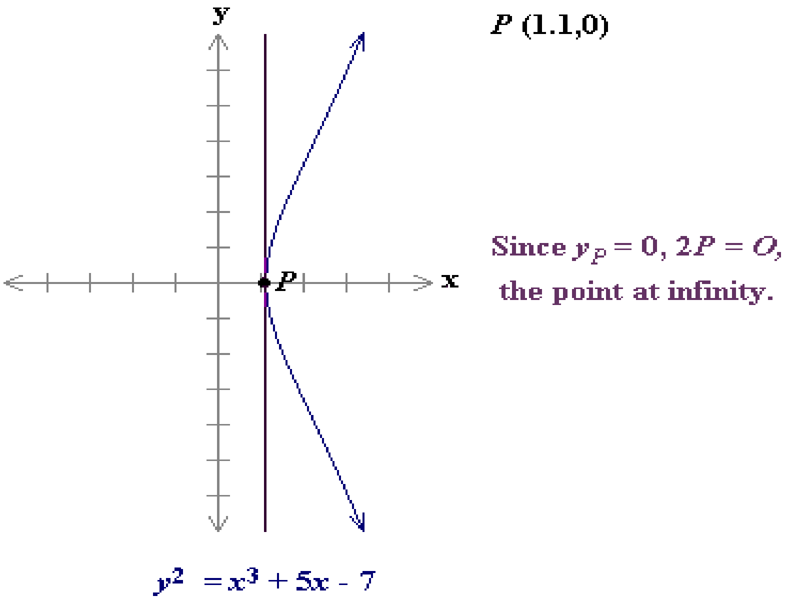


Figure 10. *Elliptic Curve with Point P: Multiplicity 3*

Example of Basic ECC Implementation

An essential property for cryptography is that a group has a finite number of points; thus, the elliptic curve's underlying field will consist of elements that form a lattice. This is due to the absolute necessity of speed and arithmetic precision in ensuring a secure system. This also explains why a field defined over the set of real numbers would be ineffective: calculations there are slow and inaccurate due to round-off error.

Recall that the field F_p contains the set of numbers from 0 to (p – 1), and computations end by taking the remainder on division by p. For example, in F_{23} the field is composed of integers from 0 to 22, and any operation within this field will result in an integer also between 0 and 22.

An elliptic curve with the underlying field of F_p can formed by choosing the variables a and b within the field of F_p. The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation modulo p (where x and y are numbers in F_p).
For example:

$$y^2 \bmod p = x^3 + ax + b \bmod p$$

has an underlying field of F_p if a and b are in F_p.

If $x^3 + ax + b$ contains no repeating factors (or, equivalently, if $4a^3 + 27b^2 \bmod p$ is not 0), then the elliptic curve can be used to form a group. An elliptic curve group over F_p consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity. There are finitely may points on such an elliptic curve.

As a very small example, consider an elliptic curve over the field F_{23}. With a = 1 and b = 0, the elliptic curve equation is $y^2 = x^3 + x$. The point (9,5) satisfies this equation since:

$$y^2 \bmod p = x^3 + x \bmod p$$

$$25 \bmod 23 = 729 + 9 \bmod 23$$

$$25 \bmod 23 = 738 \bmod 23$$

$$2 = 2$$

The 23 points which satisfy this equation are:

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15)

(17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)

These points may be graphed as

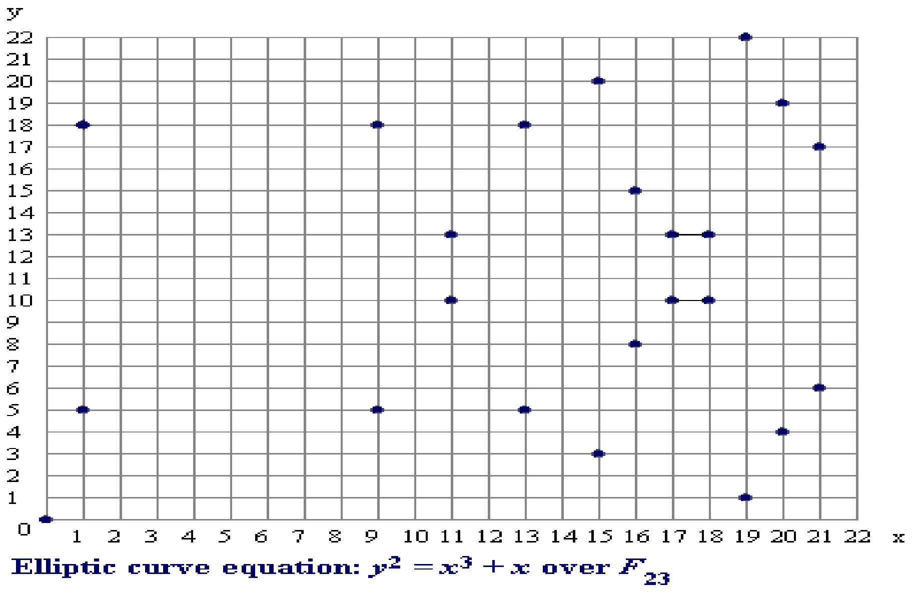


Figure 11. *Elliptic Curve Equation:* $y^2 = x^3 + x$ *over* F_{23}

Note that there is two points for every x value. Even though the graph seems random, there is still symmetry about y = 11.5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. Over the field of F_{23}, the negative components in the y-values are taken modulo 23, resulting in a positive number as a difference from 23. Here -P = (x_P, ($-y_P$ Mod 23)).

There are several major differences between elliptic curve groups over F_p and over real numbers. Elliptic curve groups over F_p have a finite number of points, which is an essential property for cryptography. Since these curves consist of a few discrete points (see the previous graph), it is not clear how to "connect the dots" to make their graph look like a curve. It is not clear how geometric relationships can be applied. As a result, the geometry used in elliptic curve groups over real numbers cannot be used for elliptic curve groups over F_p. However, the algebraic rules for the arithmetic can be adapted for elliptic curves over F_p. Unlike elliptic curves over real numbers, computations over the field of F_p involve no round off error - an essential property required for a cryptosystem.

Elements of the field F_2m are m-bit strings. The rules for arithmetic in F_2m can be defined by either polynomial representation or by optimal normal basis representation. Since F_2m operates on bit strings, computers can perform arithmetic in this field very efficiently.

An elliptic curve with the underlying field F_2m is formed by choosing the elements a and b within F_2m (the only condition is that b is not 0). As a result of the field

F_2m having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation:

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

The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over F_2m (where x and y are elements of F_2m). An elliptic curve group over F_2m consists of the points on the corresponding elliptic curve, together with a point at infinity, O. There are finitely many points on such an elliptic curve.

As a very small example, consider the field $F_2 4$, defined by using polynomial representation with the irreducible polynomial $f(x) = x^4 + x + 1$.
The element g = (0010) is a generator for the field . The powers of g are:

$$g^0 = (0001)\ g^1 = (0010)\ g^2 = (0100)\ g^3 = (1000)\ g^4 = (0011)\ g^5 = (0110)$$
$$g^6 = (1100)\ g^7 = (1011)\ g^8 = (0101)\ g^9 = (1010)\ g^{10} = (0111)\ g^{11} = (1110)$$
$$g^{12} = (1111)\ g^{13} = (1101)\ g^{14} = (1001)\ g^{15} = (0001)$$

In a true cryptographic application, the parameter *m* must be large enough to preclude the efficient generation of such a table otherwise the cryptosystem can be broken. In today's practice, *m* = 160 is a suitable choice. The table allows the use of generator notation (g^e) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without reference to the irreducible polynomial

$$f(x) = x^4 + x + 1.$$

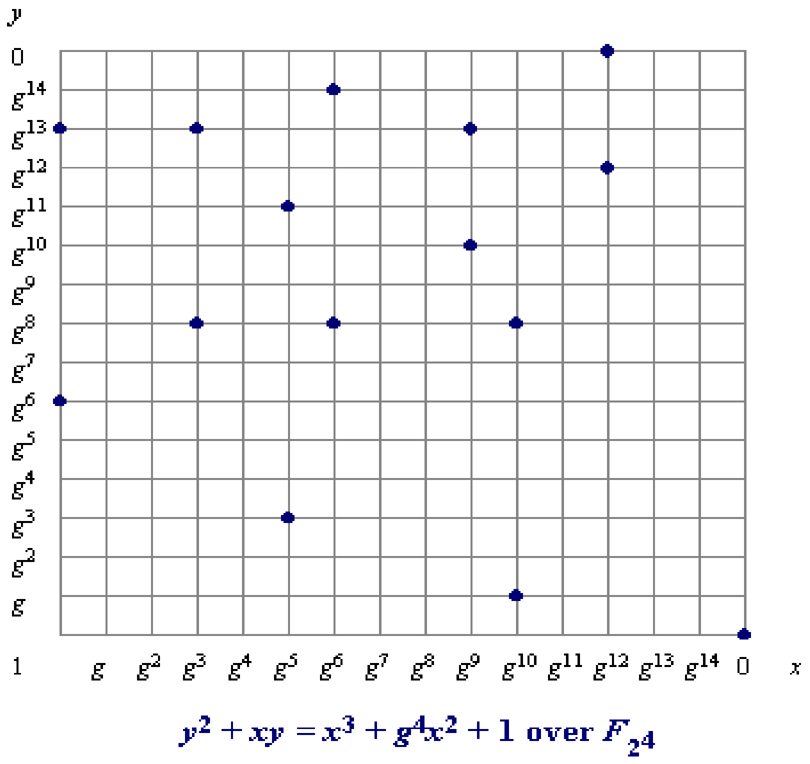


Figure 12. *Elliptic Curve $y^2 + xy = x^3 + g^4x^2 + 1$ over F_{2^4}*

At the foundation of every cryptosystem is a hard mathematical problem that is computationally infeasible to solve. The discrete logarithm problem is the basis for the security of many cryptosystems including the Elliptic Curve Cryptosystem. More specifically, the ECC relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Elliptic Curve Groups and the Discrete Logarithm Problem

Lying at the foundation of cutting-edge cryptography is the Discrete Logarithm Problem. It is this logarithm that encrypts the data and safe-guards it from attack. It is so effective that it is used in almost all cryptographic constructions, including key exchange, encryption, digital signatures, and hash functions (Silverman, 2006). It relies on the natural group law on a non-singular elliptic curve which allows one to add points on the curve together. Given an elliptic curve E over a finite field F, a point on that curve, P, and another point you know to be an integer multiple of that point, Q, the "problem" is to find the integer n such that nP=Q.

The problem is computationally difficult unless the curve has collections of numbers of points in the field which make the DLP breakable. For example, if the number of points on E over F is the same as the number of elements of F, then the curve is vulnerable to attack. It is because of these issues that point-counting on elliptic curves is such a hot topic in elliptic curve cryptography (www.planetmath.org).

CHAPTER IV

CURVES: 4^{rd} DEGREE – THE QUARTIC

Introduction

For hundreds of years, mathematicians sought some generalization of the classical formulas that would give the roots of any polynomial. Finally, P. Ruffini (1765 – 1822), in 1799, and Niels Henrik Abel (1802 – 1820), in 1824, proved that no such formula exists for the general quintic. Evariste Galois (1811 – 1832) was able to determine precisely those polynomials whose roots can be found (and, in doing so, founded the theory of groups).

History and Development of Solutions

The solution to quartic equations (and indeed, any equation of degree $\geq$ 3) has long been a focus of mathematicians and philosophers, dating from the time of the ancient civilizations. One of the earliest pieces of work on this subject is by Omar Khayyam (1048 – 1123), an Islamic mathematician, astronomer, and poet who discovered a method of solving cubics by intersecting a parabola with a circle.

The mathematician credited with first discovering a formula for finding the roots to a quartic equation was Lodovico Ferrari (1522 – 1565). Ferrari was born in Bologna, and at the age of fourteen, he was sent to Milan to work with Cardano, from whom he learned mathematics. Even at this early age, Ferrari proved to have natural ability in mathematics, and Cardano took him on as his assistant. In answer to a question posed to Cardano, Ferrari discovered a method for finding the roots to a quartic polynomial which proved to be applicable to all cases. "A new phase of mathematics began in Italy around 1500," and we first see the quartic equation discussed. Though the quartic was discussed in books during this time, it was Lodovico Ferrari who was credited for being the first to solve the quartic. In Ferrari's solution of the case:

$$x^4 + px^2 + qx + r = 0,$$

we first complete the square to obtain

$$x^4 + 2px^2 + p^2 = px^2 - qx - r + p^2.$$

For any *y* we have

$$(x^2 + p + y)^2$$

$$= px^2 - qx - r + p^2 + 2y(x^2 + p) + y^2$$

$$= (p + 2y)x^2 - qx + (p^2 - r + 2py + y^2). \quad (1)$$

With more arithmetic and in rewriting the equation as

$$(q^2 - 4p^3 + 4pr) + (-16p^2 + 8r)y - 20py^2 - 8y^3 = 0$$

to see that it is cubic in y. We know how to solve cubics and in solving for y and using this value, the right hand side of (1) is a perfect square and in taking the square root of both sides, we obtain a quadratic in x. This quadratic is solved and thus we have the required solution to the quartic equation.

About the same time frame, Rene Descartes (1656 – 1650) discovered a similar method for solving quartic equations. From those initial discoveries, several distinguished mathematicians have created their own unique formulas for solving quartic equation, including Euler, LaGrange, Bernoulli, and Klein.

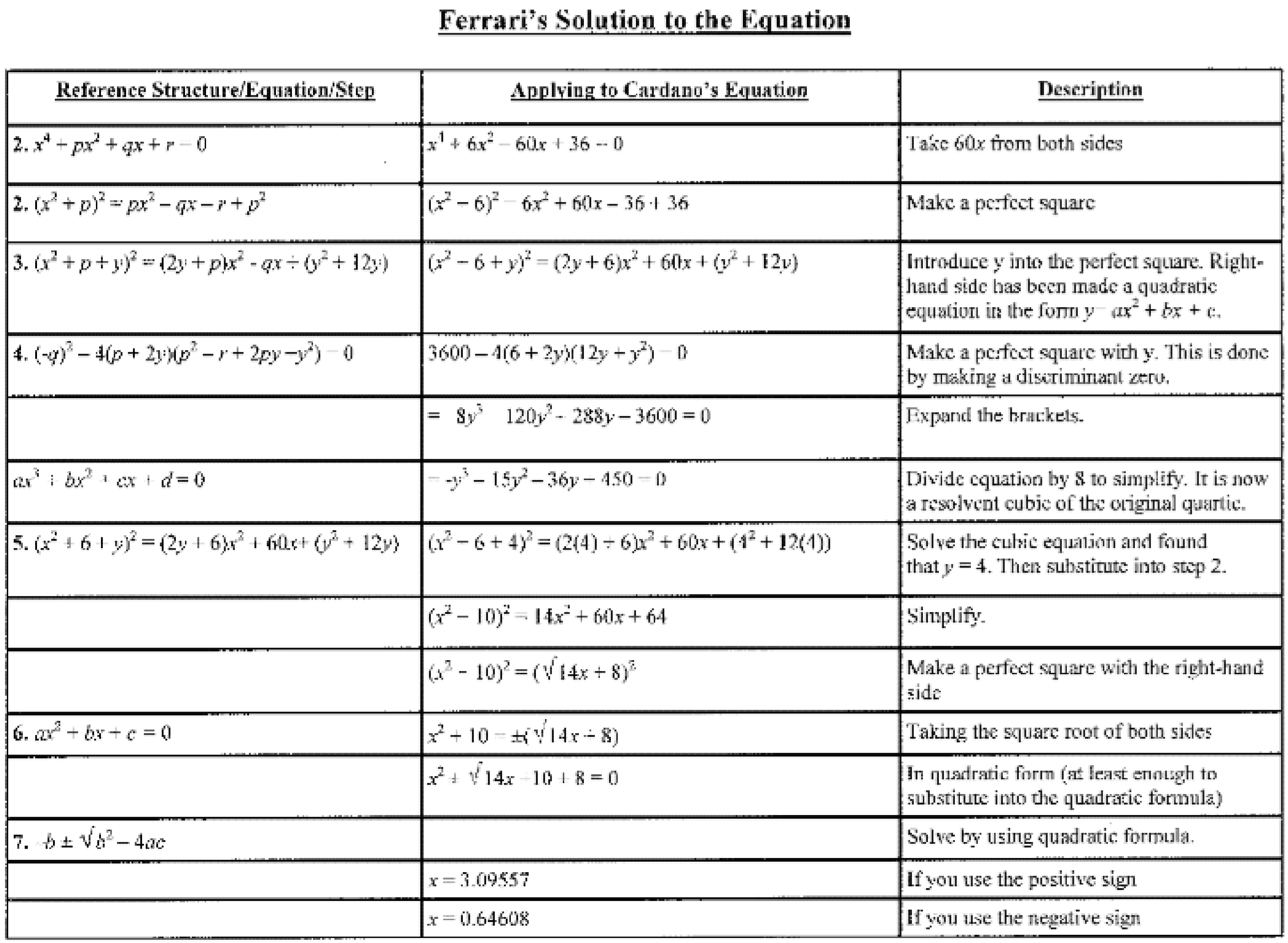
Ferrari's Discovery

Though the quartic was discussed in books during this time, it was Lodovico Ferrari who was credited for being the first to solve the quartic. The following story highlights what Ferrari is recognized to have achieved.

During Ferrari's tenure as Cardano's assistant, Cardano was given a word problem by another mathematician. "Cardano was unable to solve it. He then passed it onto Ferrari who managed to solve it. It is almost a quartic equation ($ax^4 + bx^3 + cx^2 + dx + e = 0$) except for the fact that it does not have a 'bx^3' term in it. This makes it a depressed quartic" (O'Connor and Robertson, 2011).

Table 2.

Ferrari's Solution to the Equation (courtesy of www.tripod.com)



Ferrari's Solution to the Equation

Reference Structure/Equation/Step	Applying to Cardano's Equation	Description
2. $x^4 + px^2 + qx + r = 0$	$x^1 + 6x^2 - 60x + 36 = 0$	Take $60x$ from both sides
2. $(x^2 + p)^2 = px^2 - qx - r + p^2$	$(x^2 - 6)^2 = 6x^2 + 60x - 36 + 36$	Make a perfect square
3. $(x^2 + p + y)^2 = (2y + p)x^2 - qx + (y^2 + 12y)$	$(x^2 - 6 + y)^2 = (2y + 6)x^2 + 60x + (y^2 + 12y)$	Introduce y into the perfect square. Right-hand side has been made a quadratic equation in the form $y = ax^2 + bx + c$.
4. $(-q)^2 - 4(p + 2y)(p^2 - r + 2py - y^2) = 0$	$3600 - 4(6 + 2y)(12y + y^2) = 0$	Make a perfect square with y. This is done by making a discriminant zero.
	$= \; 8y^3 \quad 120y^2 - 288y - 3600 = 0$	Expand the brackets.
$ax^3 + bx^2 + cx + d = 0$	$= -y^3 - 15y^2 - 36y - 450 = 0$	Divide equation by 8 to simplify. It is now a resolvent cubic of the original quartic.
5. $(x^2 + 6 + y)^2 = (2y + 6)x^2 + 60x + (y^2 + 12y)$	$(x^2 - 6 + 4)^2 = (2(4) + 6)x^2 + 60x + (4^2 + 12(4))$	Solve the cubic equation and found that $y = 4$. Then substitute into step 2.
	$(x^2 - 10)^2 = 14x^2 + 60x + 64$	Simplify.
	$(x^2 - 10)^2 = (\sqrt{14}x + 8)^2$	Make a perfect square with the right-hand side
6. $ax^2 + bx + c = 0$	$x^2 + 10 = \pm(\sqrt{14}x + 8)$	Taking the square root of both sides
	$x^2 + \sqrt{14}x - 10 + 8 = 0$	In quadratic form (at least enough to substitute into the quadratic formula)
7. $-b \pm \sqrt{b^2 - 4ac}$		Solve by using quadratic formula.
	$x = 3.09557$	**If** you use the positive sign
	$x = 0.64608$	**If** you use the negative sign

Descartes' Discovery

Rene Descartes discovered a method for solving a quartic at around the same time as Ferrari. His solution of the quartic was to factor a reduced quartic polynomial as a product of quadratic polynomials with real coefficients. It would then become possible to find the quartic's roots by applying the quadratic formula to its quadratic factors.

Descartes depresses the quartic by removing the x^3 term. He then tries to find *t*, *u*, and *v* such that

$$(x^4 + px^2 + qx + r) = 0 = (x^2 - tx + u)(x^2 + tx + u)$$

By comparing coefficients, he gets:

1) $u + v - t^2 = p$ 2) $t(u - v) = q$ and 3) $uv = r^{10}$

If we rewrite the first and second equations in terms of *u* and *v*, we will get

$$u + v = t^2 + p \text{ and } u - v = \frac{q}{t}$$

Solving by Gaussian elimination, we can simplify to get expressions for 2*u* and 2*v*, such that

$$2u = (t^2 + p + \tfrac{q}{t}) \text{ and } 2v = (t^2 + p - \tfrac{q}{t})$$

Therefore, based on equation 3, $(2u)(2v) = 4r$:

$$(t^2 + p + \frac{q}{t})(t^2 + p - \frac{q}{t})$$

When we simplify, we get a cubic equation in the variable t^2. Therefore, we are down to two quadratic equations which can easily be simplified.

Euler’s Discovery

Leonhard Euler was arguably one of the greatest mathematicians of all time. Publishing over 900 works in various areas, his contributions has a decisive influence over the development of mathematics, one which is still being felt to this day.

In the field of quartic solutions, Euler’s accomplishment took Descartes’ method a step further. Euler refined his method to obtain a formula for quartic solutions in terms of the solutions of the associated resolvent cubic equation. In essence, Euler’s quartic solution proved that each of the roots of a reduced quartic can be represented as the sum of three square roots, where the radicands of these square roots are the solutions of the resolvent cubic (Nickalls, 2009).

Klein’s Discovery

Felix Klein is most well-known for his work in non-Euclidean geometry, group theory and function theory. Non-Euclidean geometry allows two parallels through any external point where we see curved surfaces and thus hyperbolic and elliptic geometries. He was born April 4, 1849 and “delighted in pointing out that each of the day (5^2), month

(2^2), and year (43^2) was the square of a prime" (O'Connor and Robertson, 2003). He was intending to become a physicist, and after graduation, studied mathematics and physics at the University of Bonn. In his college years at Bonn, he worked under Plücker and upon Plücker's death, continued his major work on the foundations of line geometry. His career was in teaching mathematics and he taught a variety of courses. One of his first mathematical discoveries was investigations of W-curves which are curves invariant under a group of transformations. By 1871, he had made several major discoveries in geometry. Klein published several papers "in which he showed that it was possible to consider Euclidean geometry and non-Euclidean geometry as special cases a projective surface with a specific conic section adjoined" (O'Connor and Robertson, 2003). This led to the corollary that non-Euclidean geometry was consistent if and only if Euclidean geometry was consistent. Klein considered his work in function theory to be his most prominent contribution to mathematics. Klein studied that properties of a space are invariant under a given group of transformations and "showed how the essential properties of a given geometry could be represented by the group of transformations that preserve those properties" (O'Connor and Robertson, 2003). He did much work in developing mathematician Bernhard Riemann's ideas and obtained an explicit representation of a Riemann surface showing its equation to be $x^3y + y^3z + z^3x = 0$ as a curve in projective space. Klein then "considered equations of degree greater than 4 and was particularly interested in using transcendental methods to solve the general equation of the fifth degree" (O'Connor and Robertson, 2003).

Klein’s quartic is formed by taking regular heptagons where three meet at each corner. This creates a tiling of the hyperbolic plane and is saddle-shaped at every point. By curling up a portion of this figure, we get a 3-holed torus and it takes exactly 24 heptagons and thus Klein’s quartic. It is symmetrical with 168 symmetries (336 including reflections). In his original 1879 paper, Klein “drew a surface tiled by 24 heptagons, together with directions for how to create a 3-holed torus by attaching the sides of this surface to each other” (Figure 13). (Baez, 2013)

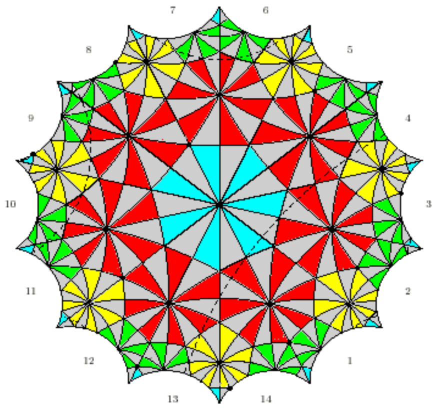


Figure 13. *Two-Dimensional Klein Quartic*.

Summary of Solution Development

In summary, any polynomial equation of degree ≤ 4 is solvable with the given conditions: the polynomial must have real number coefficients, and the solution must lie within the field of complex numbers. The method of solution would be determined by the polynomial; i.e., if direct solution is impractical, then an alternate method can be utilized. Examples of alternate methods include the Rational Root Theorem, Descartes' Rule of Signs, or the Newton Approximation Method (Villanueva, 2013).

Applications

Like its cubic cousin, the quartic polynomial has many applications and uses in our modern day world. In the field of science, many discoveries can be *described* by quartic polynomials. For example, the flow of a fluid through a tube can be modelled as a quartic function. The rate of flow of the fluid through the tube varies with the radius of the tube to the 4th degree. So if you triple the radius of a tube, 81 times more fluid can pass through the tube during an equivalent period of time (3^4 = 81). This formula, known as Poiseuille's Law, states that the laminar flow of a fluid (liquid or gas) along a pipe is given by

$$\mathrm{V} = \frac{\pi p r^4}{8nl}$$

where V = the flow rate; p = the pressure gradient between the two ends of the pipe; r = the radius of the pipe; 1 = the length of the pipe; 7 = the viscosity of the fluid (Pfitzner, 1976).

Other scientific discoveries can be modelled by quartic polynomials; one is from an area that is near and dear to me: astronomy. In fact, there are many discoveries in the field of astronomy which can be described by quartics; the one that I shall focus on is planetary orbit. In a paper presented at the International Mathematical Forum in 2008, Takuma Kimura of Hirosaki University revealed how the curve that Johannes Kepler assigned to the orbit of Mars was not a rational curve, but was instead modelled perfectly by a quartic elliptic curve.

Per Kimura, plane algebraic curves have provided various models of the orbits of planets. Curves such as hypotrochoids (roulette-type curves) provide a good representation of the orbits of inner solar system planets. Curves such as these are rational curves. Many researchers believe that Johannes Kepler supposed an ”ovoid” also explained Mars’s orbit before discovering that an ellipse modeled the true orbit of Mars.

Kepler was assigned to study the orbit of Mars by Tycho Brahe (1546-1601), when Kepler joined him in Prague around 1600. The orbit of Mars was of particular interest to study, for four reasons: it is an outer planet (and therefore seldom viewed close to the Sun); the noncircular nature of its path is the greatest of the outer planets; it is the nearest to the Earth of the outer planets (so changes in position appear larger); and it is the nearest to the Sun of the outer planets (and therefore it makes more frequent circuits, producing more observations) (O’Connor and Robertson, 2006).

CHAPTER V

CONCLUSION

The Quintic – 5th Degree Polynomials

Unlike the aforementioned linear, quadratic, cubic, or quartic equations, there exists no general formula for the solution of quintic equations (or indeed, any equation of degree ≥ 5). This, however, does not imply that no solutions exist to quintic equations. The Fundamental Theorem of Algebra tells us that every polynomial of degree *n* will have *exactly n* roots, if we count both real and complex roots, and each distinct root counted according to its multiplicity (Farouki, 2008).

Limitations

There exist very few published results on the theory of solutions to quintic equations. Further research into the solution and applications of quintics would be an appropriate extension of this thesis.

REFERENCES

Ash, Avner, and Robert Gross. *Elliptic Tales: Curves, Counting, and Number Theory*. Princeton: Princeton University Press, 2012.

Baez, John. "Klein's Quartic Curve". University of California, Riverside. Riverside, CA. May 23, 2013.

Dieudonne, Jean. *History of Algebraic Geometry: An Outline of the History and Development of Algebraic Geometry*. Montgomery: Wadsworth Advanced Books and Software, 1985. Print.

Farouki, Rida. *Pythagorean-Hodograph Curves: Algebra and Geometry Inseparable*. New York: Springer, 2008. Print.

Irving, Ronald S. "Beyond the Quartic Formula". The Mathematical Association of America, June 25, 2013.

McClendon, David. "Cubic Equations". Swarthmore College, Swarthmore, PA. 2011.

Nickalls, RWD. "The quartic equation: invariants and Euler's solution revealed". The Mathematical Gazette, March, 2009.

O'Connor, JJ and Robertson, EF. "Felix Christian Klein". 2003. http://www-history.mcs.st-andrews.ac.uk/Biographies/Klein.html

O'Connor, JJ and Robertson, EF. "Quadratic, Cubic and Quartic equations". *The MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, JOC/EFR February 1996.

Petrov, Yordan. "The solutions of cubic and quartic equations – 1". (n.d.). Retrieved From www.math10.com .

Pfitzner, J. "Poiseuille and his law". Aesthesia, 1976.

Rice, Adrian, and Brown, Ezra. "Why Ellipses Are Not Elliptic Curves". The Mathematical Association of America. 2012.

Shaw, George Bernard. *Back to Methuselah,* act I, *Selected Plays with Prefaces,* vol. 2, p.7. 1949.

Shmakov, Sergei. "A Universal Method of Solving Quartic Equations". Saratov State University, Saratov, Russian Federation, June 2, 2011.

Silverman, Joseph. "An Introduction to the Theory of Elliptic Curves". Brown University. June 19, 2006.

Szendroi, Balazs. "Cubic curves: a short survey". University of Utrecht, Utrecht, The Netherlands. January, 2005.

Villanueva, J. "The Cubic and Quartic Equations in Intermediate Algebra Courses". The Mathematical Association of America, June 25, 2013.

Weston, Harley. "Why are satellite dishes parabolic?" http://mathcentral.uregina.ca/RR/database/RR.09.95/weston1.html

ECC Tutorial. (nd.). Retrieved from

www.certicom.com.

Elliptic Curve Cryptography. 2013. Retrieved from

www.planetmath.org.

Part 4: The Cubic and Quartic From Bombelli to Euler. University of Kentucky Department of Mathematics. http://www.ms.uky.edu/~sohum/ma330/files/eqns_4.pdf. Web.

Parabolic Skis vs Straight Skis. Retrieved from

www.parabolicskis.com. 2009.

The Impossibility of Solving General Quintics in Radicals. (n.d.). Retrieved from

http://library.wolfram.com/examples/quintic/main.html