Summer 2021

Elliptic curves and their Practical Applications

Henry H. Hayden IV
Missouri State University, Hayden118@live.missouristate.edu

As with any intellectual project, the content and views expressed in this thesis may be considered objectionable by some readers. However, this student-scholar's work has been judged to have academic value by the student's thesis committee members trained in the discipline. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

Recommended Citation

Hayden, Henry H. IV, "Elliptic curves and their Practical Applications" (2021). *MSU Graduate Theses*. 3656.
https://bearworks.missouristate.edu/theses/3656

ELLIPTIC CURVES AND THEIR PRACTICAL APPLICATIONS

A Master's Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

Henry H. Hayden IV

July 2021

ELLIPTIC CURVES AND THEIR PRACTICAL APPLICATIONS

Mathematics

Missouri State University, July 2021

Master of Science

Henry H. Hayden IV

ABSTRACT

Finding rational points that satisfy functions known as elliptic curves induces a finitely-generated abelian group. Such functions are powerful tools that were used to solve Fermat's Last Theorem and are used in cryptography to send private keys over public systems. Elliptic curves are also useful in factoring and determining primality.

KEYWORDS: elliptic curves, Fermat's Last theorem, elliptic curve crpytography, congruent number problem, Hardy-Ramanujan number, elliptic curve factoring

ELLIPTIC CURVES AND THEIR PRACTICAL APPLICATIONS

By

Henry H. Hayden IV

A Master's Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

Approved:

Les Reid, Ph.D., Thesis Committee Chair

Mark Rogers, Ph.D., Committee Member

Richard Belshoff, Ph.D., Committee Member

Julie Masterson, Ph.D., Dean of the Graduate College

In the interest of academic freedom and the principle of free speech, approval of this thesis indicates the format is acceptable and meets the academic criteria for the discipline as determined by the faculty that constitute the thesis committee. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

ACKNOWLEDGEMENTS

My eternal thanks goes to Dr. Les Reid for introducing this topic to me and taking the time to explain the base concepts. Without him, I could not have completed this project. I also would like to thank Dr. William Bray for admitting me to this program and allowing me to work as a TA at MSU. Thanks is extended also to my wife and son who have supported me in this whole endeavor. Truly, this whole experience is an answer to prayer.

I dedicate this thesis to my wife, Cassie.

TABLE OF CONTENTS

1 Introduction 1

2 History of Elliptic Curves 2

2.1 The Starting Point . . . 2

2.2 From Ellipses to Elliptic Integrals . . . 3

2.3 Elliptic Integrals to Elliptic Functions to Elliptic Curves . . . 4

2.4 Chord and Tangent method . . . 6

3 Projective Planes 9

3.1 History . . . 9

3.2 Homogeneous Coordinates and the Projective Plane . . . 10

3.3 Homogeneous Polynomials and Homogenization . . . 12

3.4 Points at Infinity . . . 15

4 The Group Law 17

4.1 Singular Curves, Elliptic Curves . . . 17

4.2 Weierstrass Form . . . 17

4.3 Definition of Point Addition . . . 21

4.4 Group Law Theorem . . . 24

4.5 Theorems on Group Structure . . . 28

5 Examples 32

5.1 Examples Over the Rationals . . . 32

5.2 An Example Over a Finite Field . . . 39

5.3 Finding the Order of a Group . . . 41

5.4 Applications . . . 44

6 Elliptic Curve Factoring 55

6.1 Some Methods of Factorization . . . 55

6.2 Elliptic Curve Factorization . . . 60

6.3 Primality Testing . . . 64

7 Elliptic Curve Cryptography 68

7.1 Introduction and Definitions . . . 68

7.2 Types of Cryptographic Systems . . . 68

7.3 Logarithm Problems . . . 72

7.4 Attacks on DLP and ECDLP . . . 72

7.5 Key Exchange/Encryption . . . 84

7.6 Digital Signatures . . . 86

7.7 The Elliptic Curve Cryptography (ECC) Advantage . . . 87

8 Conclusion 89

List of Tables

5.1 Group Isomorphisms 41

5.2 Baby Steps for Determining Point Order 43

5.3 Giant Steps for Determining Point Order 43

6.1 Quadratic Sieve Congruences 59

7.1 Baby Steps of BSGS Attack 76

7.2 Giant Steps of BSGS Attack 77

7.3 Iterations of Pollard's Rho Method 80

7.4 Multiples of $38P$ for Pohlig-Hellman Attack 84

List of Figures

2.1 Pictures of Ellipses 3

2.2 Elliptic curves of different shapes 8

3.1 Perspective on Parallel lines in the distance 10

3.2 The plane $z = 1$ one unit above the origin 12

3.3 Lines through the origin intersect $z = 1$ in one point 13

3.4 Viewing the plane $z = 1$ as the affine plane 13

4.1 Nonsingular curves 18

4.2 Singular Curves 18

4.3 Adding Points on Elliptic Curves 22

5.1 Chord-Tangent Method with reflection 32

5.2 $y^2 = x^3 + 1$ 34

5.3 $x^3 + y^3 + 1 = 5xy$ 36

5.4 $x^3 + y^3 + 1 = 6xy$ 38

5.5 $y^2 = x^3 - 225x$ 51

1. INTRODUCTION

Given a certain cubic equation, we want to find rational points that satisfy the equation and to find as many of these solutions as possible. In this paper, we will explore the problem of finding rational solutions on generic cubics. We will then explore finding rational solutions of cubics in a specific form (elliptic curves). Here we will see that the geometry of the specified form lends itself to easily define an operation of “adding points on a curve.”

We will see how the addition of points and elliptic curve theory in general arose from some classic problems and how the operation of point addition is applied in those cases.

We also will see how elliptic curves were used to solve Fermat’s Last Theorem and their connection to one of the outstanding Millenial Problems, the Birch-Swinnerton-Dyer conjecture. We will then turn our attention to how point addition is applicable in the problem of integer factorization and testing for primality.

Lastly, we will see that the operation of point addition and extracting the factor of multiplication is similar to the hardness of the integer factorization problem and the discrete logarithm problem. The hardness of the problem allows these elliptic curves in certain settings to be used in cryptography settings where the problem is deemed intractable.

2. HISTORY OF ELLIPTIC CURVES

The terms elliptic curve and ellipse sound synonymous. It were as to say that elliptic curves is just another way to say ellipse. While it is true that both curves share the same word-base, it turns out that the curves are different classes and have very different properties, with elliptic curves having the more interesting and useful properties. The term elliptic curve owes its name to the fact that it arises from an ellipse, but maybe not in a way that one might expect.

2.1. The Starting Point

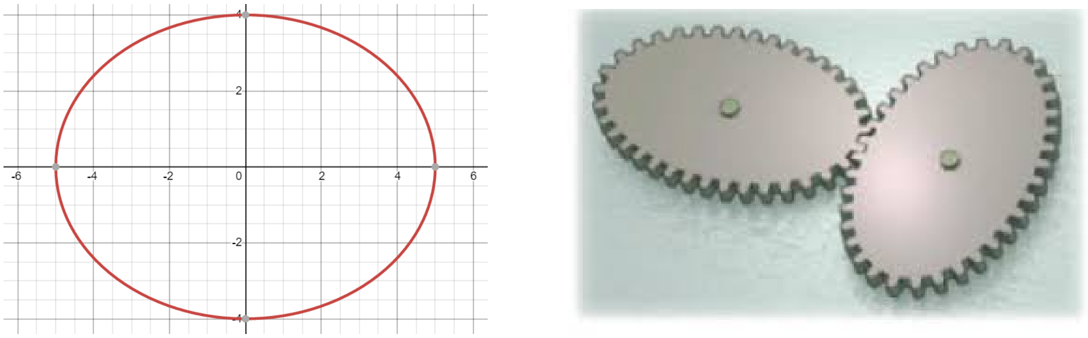
Consider the general form of an ellipse, a quadratic in terms of x and y given by

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0.$$

With a change of variables and rotation of axes, we can consider the same curve in a standard form given by

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1. \tag{2.1}$$

This is an ellipse centered at the origin of the xy-plane and if $|a| > |b|$, then the ellipse has major axis a, minor axis b, and the foci located at $c = \pm\sqrt{a^2 - b^2}$. Figure 2.1a shows an ellipse whose equation is $x^2/25 + y^2/16 = 1$ and its foci are located at $(-3, 0)$ and $(3, 0)$. Ellipses have the well-known property that the sum of the distances starting from one locus to a point on the curve and then to the other locus is equal for all points on the curve. Ellipses are useful for focusing energy waves, studying the motions of celestial bodies, for varying rotational speeds in gears (Fig. 2.1b), etc.



(a) $1 = \frac{x^2}{25} + \frac{y^2}{16}$

(b) Elliptic Gears

Figure 2.1: Pictures of Ellipses

2.2. From Ellipses to Elliptic Integrals

The formula for arclength L of a continuous, differentiable curve f on interval x_1 to x_2 is given by

$$L_{x_1}^{x_2} = \int_{x_1}^{x_2} \sqrt{1 + (f'(u))^2}\, du. \tag{2.2}$$

Apollunius of Perga who studied and developed what was mostly known about ellipses for two millennia was unable to answer the question of the length of an arc of an ellipse. Even after the invention of calculus in 1600s, the works of Newton, Euler, and Maclaurin, could only answer the question as a sum of infinite series, notably because the integration of the arclength for an ellipse induces a non-elementary integral [15].

Observe that when solving for y in (2.1), $y = f(x) = \frac{b}{a}\sqrt{a^2 - x^2}$, thus,

$$\begin{aligned} f'(x) &= -\frac{bx}{a\sqrt{a^2 - x^2}} \\ (f'(x))^2 &= \frac{b^2x^2}{a^2(a^2 - x^2)} \end{aligned} \tag{2.3}$$

Thus we substitute Eq. (2.3) into Eq. (2.2) and use variable $x = au$

$$\begin{aligned} L &= \int_{u_1}^{u_2} a\sqrt{1 + \frac{a^2b^2u^2}{a^2(a^2 - a^2u^2)}}\, du \\ &= \int_{u_1}^{u_2} a\sqrt{\frac{a^2 - (a^2u^2 - b^2u^2)}{(a^2 - a^2u^2)}}\, du \\ &= \int_{u_1}^{u_2} \sqrt{\frac{a^2 - k^2u^2}{1 - u^2}}\, du \end{aligned}$$

where $k^2 = a^2 - b^2$.

2.3. Elliptic Integrals to Elliptic Functions to Elliptic Curves

Non-elementary integrals were studied intensely by Adrien-Marie Legendre. He came to the realization that arclength calculations could be parameterized by $u = \sin t$ and $y = b\cos t$. The arclength functions fell into one of three categories, which have become to be known as elliptic integrals of *first, second*, and *third kind*, respectively. Abel and Jacobi carried Legendre's work further by parameterizing with $x = \sin t$ and refined the three classes of integrals. Together, the three classes can be identified as F, E, and Π as the first, second, and third kinds. We give their general presentations here.

$$\begin{aligned} F(u,k) &= \int_0^u \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}, \\ E(u,k) &= \int_0^u \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\, dx \\ \Pi(u,k,n) &= \int_0^u \frac{dx}{(1+nx^2)\sqrt{(1-x^2)(1-k^2x^2)}}, \quad |u| \leq 1. \end{aligned}$$

Note that

$$F(u,0) = \int_0^u \frac{dx}{\sqrt{1-x^2}} = \sin^{-1} u,$$

the inverse sine function expressed as an integral. Jacobi considered nonzero k, and studied the inverses $F^{-1}(u,k)$, a function he called *sine amplitude* (using Legendre's term), denoted

$$\operatorname{sn} u = F^{-1}(x).$$

This is an example of an *elliptic function.*

As a result, elliptic functions then are similar to the sine function. It is well-known that the sine function is periodic with a period of 2π, that is for $n \in \mathbb{Z}$, then $\sin x = \sin(x + 2n\pi)$. Jabcobi showed that the elliptic functions are also periodic. Moreover, elliptic functions and only elliptic functions are exactly (no more than) *doubly* periodic. That is, there exists $\alpha, \beta \in \mathbb{C}$ with $\alpha/\beta \notin \mathbb{R}$ such that

$$\operatorname{sn}(u + m\alpha) = \operatorname{sn}(u + n\beta) = \operatorname{sn} u$$

for $m, n \in \mathbb{N}$ [15].

We know that the derivative of trig functions are still trig functions. Let us consider the derivatives of elliptic functions. To explore this topic further, consider the infinite series

$$\sum_{m=-\infty}^{\infty} (z + m\pi)^{-2} = (\sin z)^{-2}.$$

Elliptic functions can also be expressed in a similar power series. Let $\omega_1, \omega_2 \in \mathbb{C}$ and $m, n \in \mathbb{Z}$, define a lattice L by

$$L = \{m\omega_1 + n\omega_2\}.$$

Then let $l \in L$ for a given choice of m, n. Eisenstein showed that the elliptic function in the form

$$y(z) = \sum_{l \in L, l \neq 0} (z + l)^{-2} - \sum_{l \in L, l \neq 0} l^{-2}$$

had to satisfy a differential equation in the form of

$$[y'(z)]^2 = p(y(z))$$

for a cubic polynomial p with no repeated roots. In 1863, Karl Weierstrass proved that his

$\wp$-function defined

$$\wp(z) = \wp(z; L) := \frac{1}{z^2} + \sum_{l \in L,\, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

is doubly periodic, meromorphic function over the complex numbers, hence, an elliptic function [11]. In fact $\wp'(z)$, $\wp''(z)$ and all the derivatives of $\wp(z)$ are elliptic functions.

Just like as all of trigonometric functions can be expressed as rational functions of $\sin x$ and its derivatives, the Weierstrass $\wp$-function and its derivatives is the basis for all elliptic functions ([15] p.172).

Here, we present the modern definition of an elliptic function: a single-valued, meromorphic function f, defined over $\mathbb{C}$, for which there are two distinct complex numbers ω_1 and ω_2 such that the ratio $\omega_1/\omega_2 \notin \mathbb{R}$ such that

$$f(z+\omega_1) = f(z+\omega_2) = f(z).$$

Weierstrass proved that $\wp(z)$ satisfied a cubic differential equation, specifically

$$[\wp'(z)]^2 = 4\wp(z)^3 - g_1\wp(z) - g_2$$

with constants $g_1,\ g_2$ that depend on $\omega_1,\ \omega_2$. By letting $x = \wp(z)$ and $y = \wp'(z)$, we see a parameterization of the cubic curve

$$y^2 = 4x^3 - g_1 x - g_2.$$

These results are discussed in Koblitz [11] and in Rice and Brown [15].

2.4. Chord and Tangent method

In the 1670s, Newton used the geometry of elliptic curves to describe the method of obtaining rational points that lie on the curve. This method of obtaining rational points gives elliptic curves a structure that is not immediately observable, and took the consider-able efforts of Henri Poincaré in 1901 to pull all these ideas together [15].

Let's describe the tangent-chord method that Newton investigated.

First, if a line intersects a cubic at two points, then that line will usually intersect the cubic at a third. We can allow two or more of these points to be the same, so the line can be tangent to the curve with multiplicity 2 or 3. If the line is tangent with multiplicity 2, then the line will intersect at one other point on the cubic. If a line is tangent to the cubic with multiplicity 3, then the line will not intersect at any other point on the curve.

Notice in Figure 2.2, graphs one, two, and three represent three cubics; two are connected and one is disconnected. The tangent-chord method works for connected and disconnected elliptic curves and we need not limit our studies to solely connected or disconnected elliptic curves.

For example,

$$E(x, y) = y^2 - x^3 + 2 = 0$$

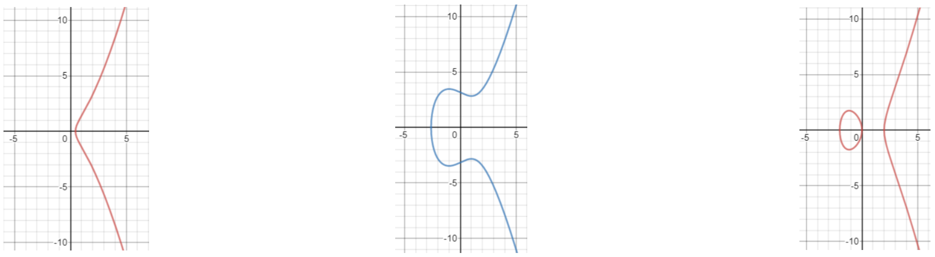
We can see that $P = (-1, 1)$ lies on E. We can find a third point on E by finding the equation of the line tangent to E at P and solving for where it intersects E again.

First we find the derivative, $2y\left(\frac{dy}{dx}\right) = 3x^2$, and plug in P. This yields $dy/dx = 3/2$. We find the y-intercept using $y = mx + b$ and using P and dy/dx, we find $b = 5/2$. Thus the equation of the line tangent to E at P is

$$y = \frac{3}{2}x + \frac{5}{2}.$$

We find where the tangent line intersects E again by taking its equation and substituting into E. We then solve for the three roots.

$$\begin{aligned}
\left(\frac{3}{2}x + \frac{5}{2}\right)^2 &= x^3 + 2 \\
\frac{9}{4}x^2 + \frac{15}{2}x + \frac{25}{4} &= x^3 + 2 \\
0 &= x^3 - \frac{9}{4}x^2 - \frac{15}{2}x - \frac{17}{4} \\
&= (x + 1)(x + 1)(x - 17/4)
\end{aligned}$$



(a) $y^2 = x^3 + 2x - 1$ (b) $y^2 = x^3 - 3x + 10$ (c) $y^2 = x^3 - 4x$

Figure 2.2: Elliptic curves of different shapes

We already know that the line was tangent at P so the first two solutions of $x = -1$ come from P. We are interested in the third solution, $x = 17/4$. We take this value and plug into E and we find $y^2 = 5041/64$ and thus $y = \pm 71/8$. Since the tangent line has positive slope we find ourselves interested in the positive value. Thus the tangent line intersects E at

$$\left(\frac{17}{4}, \frac{71}{8}\right).$$

This example will be discussed further in section 5.1.1 where we will look at the chord and tangent method after more development of the ideas presented here. But to procede, we must first discuss projective curves.

3. PROJECTIVE PLANES

3.1. History

Consider the difficulties of capturing the essence of a 3-D scene on a 2-D piece of paper or canvas. The process of fixing oneself to a point in space and capturing the observed universe onto paper is called linear perspective. One can think of it as drawing lines out from the observer's eyes to objects in the distance, insert a piece of paper somewhere between the observer and those objects, and where those lines intersect the paper is where the information is relayed onto the drawing.

Hasan Ibn al-Haytham, also known as Alhazen, wrote about perspective and optics in first century of 1000s, but his ideas were not immediately put to use. Giotto di Bondone in the late 1200s is noted to be one of the first to include perspective in his works. Artists started started using ideas on perspective regularly beginning in the 1400s. Before then, perspective on different objects was relegated by their importance, not necessarily by their relation to each other geometrically. Brunelleschi and Alberti in 1415 used similar triangles to try to capture the distance between objects. Piero della Francesco, a geometer, mathematician and artist, wrote specifically on perspective in painting (in a paper by the same name) in 1400s. His paintings are noted for his approach to perspective, notably *Brera Madonna*. In 1500s, Luca Pacioli, an Italian artist and mathematician, wrote on geometric and artistic proportion, including the use of the golden ratio in architecture. He was a contemporary of Da Vinci who illustrated some of Pacili's works. Most famously, Da Vinci used perspective to create a vanishing point in his most notable works, *Mona Lisa* and *The Last Supper*. This is a summary of art history from the websites of [12] and [23].

Notice in Figure 3.1, the use of a vanishing point in relation to the railroad tracks. Although the tracks are parallel, they appear to disappear (or merge or intersect) as we look off into the distance. We could consider these particular set of tracks to represent a family of parallel lines with a particular slope m on the xy-plane. The point where the

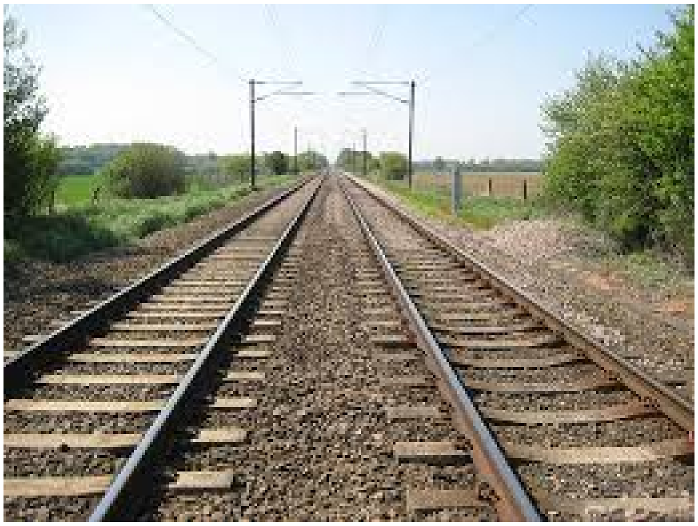


Figure 3.1: Perspective on Parallel lines in the distance

lines seem to intersect in the distance would then represent the point at infinity where all the lines of that family of slope m would intersect. Likewise, a different family of lines with a different slope m would have a vanishing point at infinity. For each family of lines of slope with $m \in \mathbb{R}$, including vertical lines that have no slope m, then there is one point at infinity for each family.

These ideas of linear perspective and intersections at infinity will motivate our discussion of projections.

3.2. Homogeneous Coordinates and the Projective Plane

An **affine plane** over a field K is defined

$$\mathbb{A}^2_K = \{(x,y)|x,y \in K\}.$$

Similarly, **affine space**, denoted $\mathbb{A}^3_K$, or just K^3, is defined

$$\mathbb{A}^3_K = K^3 = \{(x,y,z)|x,y,z \in K\}$$

Projective n-space over a field K, which is denoted $\mathbb{P}^n_K$, or simply $\mathbb{P}^n$, is the set of equivalence classes of $(n+1)$-tuples $(a_0, \ldots, a_n)$ of elements of K, not all zero, such that $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for $\lambda \in K$, $\lambda \neq 0$. In other words, $\mathbb{P}^n$ is the set of lines in $\mathbb{A}^{n+1} \backslash (0, \ldots, 0)$ going through the origin with an equivalence relation that identifies which points lie on the same line through the origin. An element of $\mathbb{P}^n$ is a point. Any point $P \in \mathbb{P}^n$ is a representative of some equivalence class, so P can represent the entire class. The representatives for the equivalence for P are the **set of homogeneous coordinates for** P. [9]

Consider the **projective plane** in the case when $n = 2$, that is, lines in K^3 going through the origin $(0, 0, 0)$ and the plane $z = 1$. Then each line intersects the affine plane $z = 1$ in a unique point. With our equivalence relation in place, this point is the representative for that equivalence class. In the case of lines in K^3 that lie solely in the xy-plane ($z = 0$), each with a different slope, these lines are equivalence classes that represent the points at infinity for families of parallel lines in $z = 1$ with the same slope. This collection of points at $z = 1$ plus the points at infinity creates the projective plane.

Homogeneous coordinates have the following properties.

1. Each line in K^3 going through the origin is an equivalence class and is denoted $(X : Y : Z)$. We exclude the origin from the set of equivalence classes to avoid ambiguity. We define the projective plane as $P^2_K = \{(X : Y : Z) | X,\ Y,\ Z \in K, (X : Y : Z) \neq (0, 0, 0)\}$.

3. Any equivalence class $(X : Y : Z)$ with $z \neq 0$ can be represented as $(X/Z, Y/Z, 1)$. For $x = X/Z$ and $y = Y/Z$, each of these projective points in $\mathbb{P}^2_K$ can be identified with affine points $(x, y) \in A^2_K$.

4. For $Z = 0$, then any point $(X : Y : 0)$ is considered a point at infinity.

Figure 3.2 captures a 3-D view of the projective plane in space. The y-axis is green extending positively to the right and negatively to the left. The x-axis is red extending positively to the foreground and negatively in the background. The z-axis is blue extend-

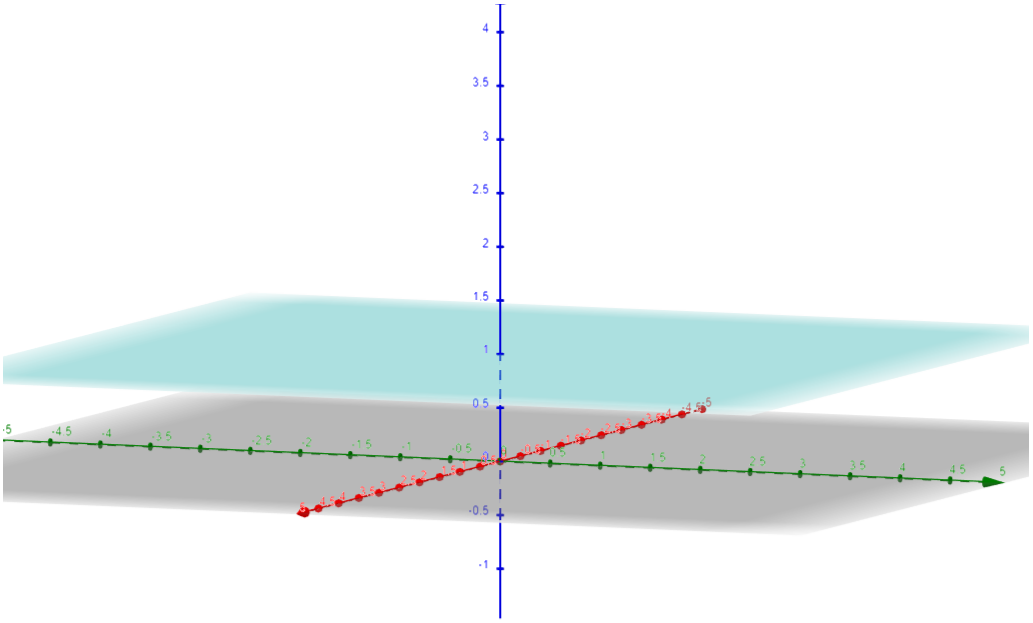


Figure 3.2: The plane $z = 1$ one unit above the origin

ing positively up and negatively down. The light gray plane is the xy-plane where $z = 0$. the light blue plane where $z = 1$ represents the projective plane.

Figure 3.3 Shows some lines through the origin and their intersections with the plane $z = 1$.

Figure 3.4 is the same as Figure 3.3 but from the perspective of looking down the z-axis so the the xy-plane is oriented as if it were the affine plane. One can see that the lines through the origin intersect the plane $z = 1$ as they extend upward away from the origin. The points $A,\ B,\ C,\ D,\ E$ are represented by the blue balls. The solid portion of the lines are the half of the lines above the plane $z = 1$; the dotted portion of the lines are the half below $z = 1$.

3.3. Homogeneous Polynomials and Homogenization

The **degree of a monomial** k is the sum of exponents of variables within the monomial. The **degree of a polynomial** F is the max d of all the degrees of terms of F.

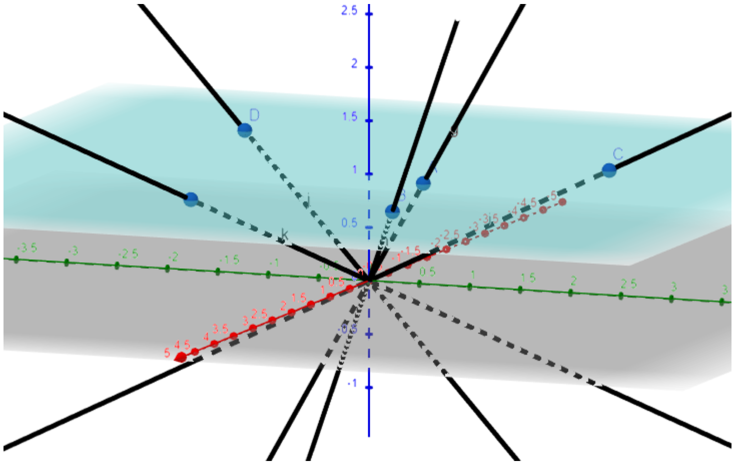


Figure 3.3: Lines through the origin intersect $z = 1$ in one point

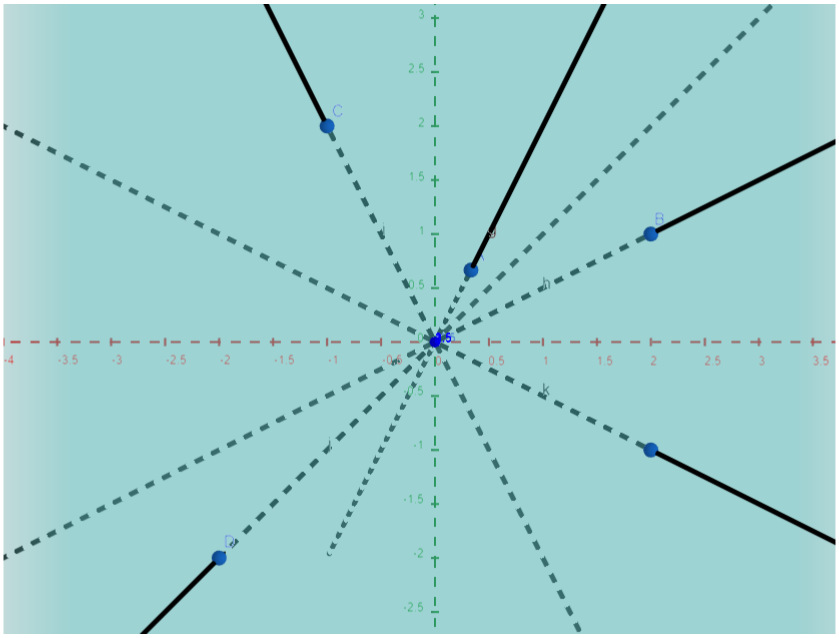


Figure 3.4: Viewing the plane $z = 1$ as the affine plane

A **homogeneous polynomial** F is a polynomial in which all terms have the same degree. A homogeneous polynomial of degree d can also be defined as one satisfying $F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z)$ for any $\lambda \in K$.

To **homogenize** a polynomial expressed in terms of x and y is to multiply each term of the polynomial by an appropriate power of Z so that the sum of the exponents in each term is d. Given some polynomial $f(x, y)$ of degree d, let F represent the the homogenized form of f given by

$$F(X, Y, Z) = Z^d f(X/Z, Y/Z).$$

Example 1. Homogenize

$$f(x, y) = x^3 + 2x^2 - y^2 - x - 5 = 0.$$

Then f is degree 3 and

$$\begin{aligned} F(X, Y, Z) &= Z^3 f(X/Z, Y/Z) \\ &= Z^3 \left[\left(\frac{X}{Z}\right)^3 + 2\left(\frac{X}{Z}\right)^2 - \left(\frac{Y}{Z}\right)^2 - \frac{X}{Z} - 5 \right] \\ &= X^3 + 2X^2Z - Y^2Z - XZ^2 - 5Z^3 = 0. \end{aligned}$$

which makes F homogeneous with degree 3.

To **dehomogenize** a homogeneous polynomial F with respect to Z is to rewrite $F(X, Y, Z)$ such that $X = x$, $Y = y$, and $Z = 1$. If $F(X, Y, Z)$ is homogeneous of degree d, then

$$f(x, y) = Z^{-d} F(X, Y, Z) = F(X/Z, Y/Z, 1) = F(x, y, 1)$$

Intuitively, this is the opposite process of homogenization where Z is “removed.”

Example 2. Dehomogenize

$$F(X, Y, Z) = X^4 - X^2Y^2 + 2XY^2Z - 3Y^3Z + 5Z^4.$$

with rexpect to Z.

Then F is homogeneous of degree 4 and we find

$$\begin{aligned} f(x,y) &= Z^{-4}F(X,Y,Z) \\ &= F\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) \\ &= \left(\frac{X}{Z}\right)^4 - \left(\frac{X}{Z}\right)^2\left(\frac{Y}{Z}\right)^2 + 2\left(\frac{X}{Z}\right)\left(\frac{Y}{Z}\right)^2 - 3\left(\frac{Y}{Z}\right)^3 + 5 \\ &= x^4 - x^2y^2 + 2xy^2 - 3y^3 + 5. \end{aligned}$$

Then f is heterogeneous of degree 4.

Notice the connection between homogeneous coordinates and homogeneous polynomials. If $(x,y,z) \sim (x',y',z')$ then by definition $(x,y,z) = (\lambda x, \lambda y, \lambda z)$ for some $\lambda \in K$. If F is a homogeneous polynomial with $F(x,y,z) = 0$, then

$$\begin{aligned} F(x',y',z') &= F(\lambda x, \lambda y, \lambda z) \\ &= \lambda^d F(x,y,z) \\ &= \lambda^d(0) \\ &= 0. \end{aligned}$$

We see then that the choice of representative of an equivalence class does not matter and F is well-defined.

3.4. Points at Infinity

Now we turn our attention to the case of the lines that lie solely in the xy-plane, the case when $Z = 0$.

In the affine plane, each family of parallel lines all have the same slope, m. Each line has equation $y = mx + b$, for some b. In projective coordinates, when $Z \neq 0$, then

$$\left(\frac{X}{Z} : m\frac{X}{Z} + b : 1\right) \sim (X : mX + BZ : Z).$$

In the case of $Z = 0$, then

$$(X : mX : 0) \sim (1 : m : 0).$$

There is one point at infinity for each family of parallel lines with slope m.

In the case of family of vertical lines, where $x = c$ for some constant c, then when $Z \neq 0$

$$\left(c : \frac{Y}{Z} : 1\right) \sim (cZ : Y : Z).$$

When $Z = 0$, then

$$(0 : Y : 0) \sim (0 : 1 : 0).$$

In general, by homogenizing and setting $Z = 0$, we can find the point at infinity for a curve.

Example 3. Consider

$$(y - 2x)(3x - y)(2x - 3y) = 1.$$

Then $f(x, y) = (y - 2x)(3x - y)(2x - 3y) - 1 = 0$. If we homogenize f, then

$$F(X, Y, Z) = (Y - 2X)(3X - Y)(2X - 3Y) - Z^3 = 0.$$

In the case of $Z = 0$, then the solutions are $(X, 2X, 0)$, $(X, 3X, 0)$, and $(3X, 2X, 0)$. These are equivalent to $(1, 2, 0)$, $(1, 3, 0)$, and $(3, 2, 0)$, so there are three points at infinity.

Example 4. Consider the equation of an elliptic curve in special form

$$y^2 = x^3 + Ax + B.$$

Then $f(x, y) = y^2 - x^3 - Ax - B = 0$. The homogenized form of f is given by

$$F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3 = 0.$$

In the case of $Z = 0$, then $X^3 = 0$, thus $X = 0$ and Y is arbitrary. Thus $(0, Y, 0) \sim (0, 1, 0)$. This shows that for equations of this form, there is one point of infinity for families of vertical lines.

4. THE GROUP LAW

4.1. Singular Curves, Elliptic Curves

Definition. A curve is **singular** at a point if its partial derivatives are simultaneously zero at that point.

In particular, a homogeneous, projective curve $F(X,Y,Z) = 0$ with $(X,Y,Z) \neq (0,0,0)$ is singular at (X,Y,Z) if

$$F(X,Y,Z) = F_X(X,Y,Z) = F_Y(X,Y,Z) = F_Z(X,Y,Z) = 0.$$

Figures 4.1 and 4.2 below show some nonsingular and singular curves.

For example, if $F(X,Y,Z) = Y^2Z - X^3 - 3X^2Z = 0$, then $F_X(X,Y,Z) = -3X^2 - 6XZ$, $F_Y = 2YZ$, and $F_Z = Y^2 - 3X^2$. Then (0,0,1) is a singular point of F. Singular points occur when curves wrap around on themselves (self-intersect or nodes) or cusps are created. Figure 4.2a shows an affine piece of the projective curve F in the affine plane, $f(x,y) = y^2 - x^3 - 3x^2 = 0$ and the point of singularity at the origin.

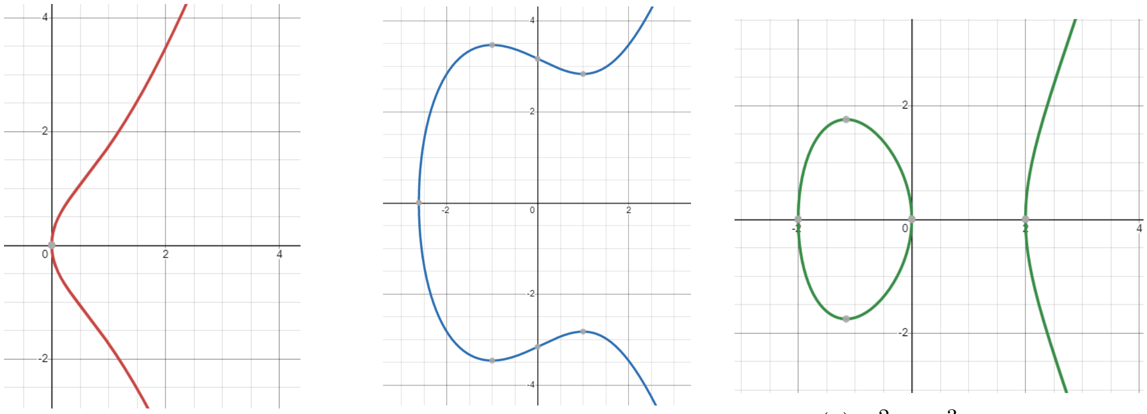
Definition. An **elliptic curve** over a field K is a projective, non-singular cubic curve with at least one rational point in K^3, also called K-rational points.

4.2. Weierstrass Form

The most general form of a cubic in terms of x and y is:

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Weierstrass was able to show that any cubic with a K-rational point can be transformed into a special form called **Weierstrass normal form**. Here, let us define these special forms and then define the group of points on an elliptic curve E.

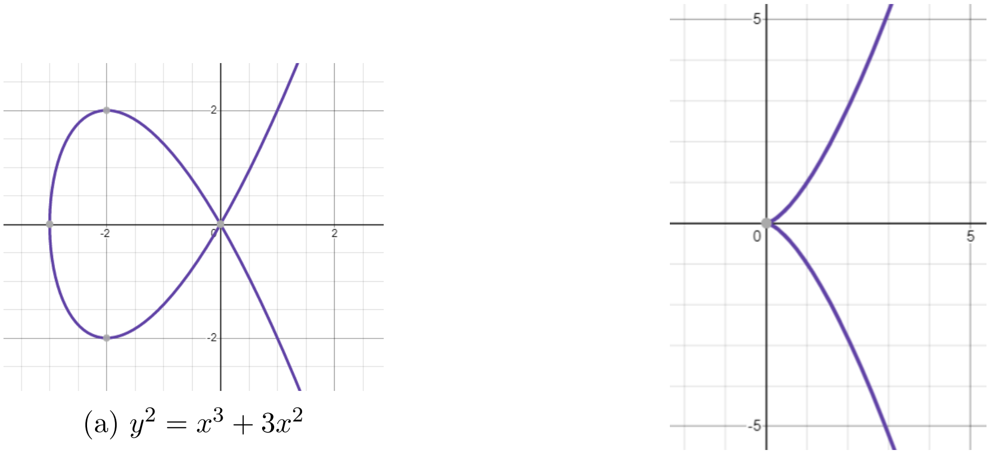


(a) $y^2 = x^3 + 2x$

(b) $y^2 = x^3 - 3x + 10$

(c) $y^2 = x^3 - 4x$

Figure 4.1: Nonsingular curves



(a) $y^2 = x^3 + 3x^2$

(b) $y^2 = x^3$

Figure 4.2: Singular Curves

Definition (Normalized Weierstrass Form)**.** A cubic in the form of

$$y^2 = x^3 + Ax + B$$

is called Normalized Weierstrass Form, or just normal form.

We note here that any cubic curve E over a field K that is not of characteristic 2 or 3 can be put in normal form.

Definition (Group of Rational Points)**.** Let E be an elliptic curve in normal form defined over $\mathbb{Q}$. Then the set of rational points on E is defined as

$$E(\mathbb{Q}) := \{\infty\} \cup \{(x, y) \in \mathbb{Q}^2 | y^2 = x^3 + Ax + B\}.$$

For fields K with char$K \neq 2, 3$, then Weierstrass normalized form, or just Weierstrass form, in projective coordinates can be written $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3 = 0$.

Since we require that elliptic curves be non-singular, we must then discuss what limitation or limitations we must put on Weierstrass form to guarantee that an elliptic curve is non-singular.

Proposition 4.2.1. *An elliptic curve in Weierstrass form is non-singular if and only if the quantity* $4A^3 + 27B^2 \neq 0$.

Proof. Since the claim is bi-conditional, we will prove the contrapositive.

$\Rightarrow$ Assume $4A^3 + 27B^2 = 0$. Then $B = \sqrt{4(-A)^3/27}$. So consider the equation

$$f(x, y) = y^2 - x^3 - Ax - \sqrt{\frac{4(-A)^3}{27}} = 0.$$

Then $f_y = 2y$ and $f_x = -3x^2 - A$. Now consider the point $P = (\sqrt{-A/3}, 0)$. Then

$$\begin{aligned} f(\sqrt{-A/3}, 0) &= 0^2 - \left(\sqrt{\frac{-A}{3}}\right)^3 - A\left(\sqrt{\frac{-A}{3}}\right) - \sqrt{\frac{4(-A)^3}{27}} \\ &= \frac{A}{3}\sqrt{\frac{-A}{3}} - A\sqrt{\frac{-A}{3}} + \frac{2A}{3}\sqrt{\frac{-A}{3}} \\ &= 0. \end{aligned} \tag{4.1}$$

Then $f_y(P) = 0$ and $f_x(P) = 3(\sqrt{-A/3})^2 + A = 0$. Thus $f(P) = f_y(P) = f_x(P) = 0$ and the curve is singular at P.

$\Leftarrow$ Assume the the curve is singular. Consider the projective, homogeneous Weierstrass form $F(X, Y, Z) = Y^2Z - G(X, Z) = 0$ where $G(X, Z) = X^3 + AXZ^2 + BZ^3$. Then consider the partial derivatives of F: $F_X = -3X^2 - AZ^2$, $F_Y = 2YZ$, and $F_Z = Y^2 - 2AXZ - 3BZ^2$.

If $F_Y = 0$, then $Y = 0$ or $Z = 0$. If $Z = 0$, $F_X = 0$ means $X = 0$. Since $F_Z = 0$, this forces $Y = 0$. This gives the point (0,0,0) which is excluded upon assumption, so we exclude the case $Z = 0$ and assume that Z is non-zero.

So then $Y = 0$. Since $Z \neq 0$, then we can dehomogenize G, and we have $g(x) = x^3 + Ax + b$, and $g'(x) = 3x^2 + A$. But since $Y = 0$ and $Y^2 = G(X, Z)$, then $g(x) = 0$ and $g'(x) = 0$ and g has multiple roots.

Consider then that when $g'(x) = 0$, then $x = \pm\sqrt{-A/3}$. Then substituting into $g(x) = 0$,

$$\begin{aligned} \left(\pm\sqrt{-\frac{A}{3}}\right)^3 + A\left(\pm\sqrt{-\frac{A}{3}}\right) + B &= 0 \\ B &= \left(-\frac{A}{3}\right)\left(\mp\sqrt{-A/3}\right) + A\left(\mp\sqrt{-A/3}\right) \\ &= \frac{2A}{3}\left(\mp\sqrt{-A/3}\right) \\ B^2 &= \frac{4A^2}{9}\cdot\frac{-A}{3} \\ 27B^2 + 4A^3 &= 0. \end{aligned}$$

□

For example, in the case of $y^2 = x^3 - 4x$, then $A = -4$, and $B = 0$, thus $4A^3 + 27B^2 = 64 \neq 0$, thus it is non-singular, as shown in Fig 4.1c.

4.3. Definition of Point Addition

We wish to put a group structure on $E(\mathbb{Q})$.

Geometrically, define point addition from the tangent-chord method where we want to find where a tangent line or a chord intersects an elliptic curve at a third point. If P and Q are two points on the curve, define the operation $\star$ as finding a third point $R' = (x_1, y_1)$ on the curve so that $P \star Q = R'$. After R' is found, find its reflection across the x-axis and define this operation as point addition $+$ so that $P + Q = R$ where $R = (x_1, -y_1)$. The line connecting points P and Q in Fig. 4.3 shows the operations of $\star$ and $+$.

We also define $P + Q = \infty$ whenever the line connecting P and Q is vertical. We use ∞ as a shorthand for $(0, 1, 0)$, which we saw earlier was the point for infinity for our elliptic curve. This is the point where all vertical lines intersect in the projective plane and we identify this as the identity element so that $P + \infty = P$ for all P on the curve.

Let E be a projective elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E. We can compute the addition of points

$$P_1 + P_2 = P_3 = (x_3, y_3)$$

into the following cases.

1. For all points P, define

$$P + \infty = P.$$

For a vertical line connecting P_1 and ∞, then the line crosses E a third time at the

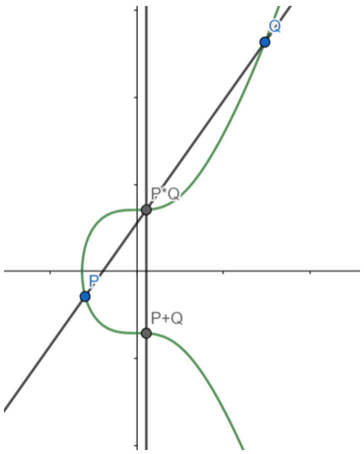


Figure 4.3: Adding Points on Elliptic Curves

reflection of P_1 across the x-axis. By definition of $\star$, we find

$$P_1 \star \infty = (x_1, -y_1),$$

so that by definition of $+$,

$$P_1 + \infty = (x_1, -(-y_1) = P_1,$$

which holds for all points P on E.

2. For $P_1 = P_2$ and $y_1, y_2 \neq 0$,

   we can find the slope of the line tangent to E by taking the derivative, finding

$$m = \frac{3x_1^2 + A}{2y_1}.$$

   We find the y-intercept b of the tangent line by $b = y_1 - mx_1$. Thus we have the equation of the line tangent to the curve $y = mx + b$. By substitution,

$$\begin{array}{rcl} (mx+b)^2 & = & x^3 + Ax + B \\ 0 & = & x^3 - m^2x^2 + \cdots \end{array}$$

Note also, that if x_1, x_2, x_3 are the roots of any cubic, then

$$\begin{aligned} 0 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + \cdots \end{aligned}$$

We can relate the two equations by setting them equal to each other. Thus

$$x^3 - (x_1 + x_2 + x_3)x^2 + \cdots = x^3 - m^2x^2 + \cdots .$$

We set the coefficients of the x^2 term equal to each other and

$$x_1 + x_2 + x_3 = m^2.$$

Since $x_1 = x_2$, then

$$x_3 = m^2 - 2x_1. \tag{4.2}$$

Therefore,

$$\begin{aligned} y_3' &= mx_3 + b \\ y_3 = -y_3' &= -(mx_3 + y_1 - mx_1) \\ &= m(x_1 - x_3) - y_1 \end{aligned}$$

3. If $x_1 = x_2$, and $y_1 = -y_2$,

   then line connecting the two points is vertical since $m = \frac{y_2+y_1}{x_2-x_1} = \frac{2y_1}{0}$. In the case $y_1 = y_2 = 0$, then $P_1 = P_2$ and $dy/dx = (3x^2 + A)/0$. Thus,

$$P_1 + P_2 = \infty.$$

4. If $x_1 \neq x_2$,

and we find the slope of the line between the two points

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Find x_3 by subtracting two known roots from m^2 so that

$$x_3 = m^2 - x_1 - x_2.$$

Find y_3 as in Case 2A:

$$y_3 = m(x_1 - x_3) - y_1.$$

4.4. Group Law Theorem

Theorem 4.4.1. *The addition of points on E satisfies the following four properties:*

1. *Commutativity: $P_1 + P_2 = P_2 + P_1$ for all P_1, P_2 on E.*
2. *Existence of Identity: $P + \infty = P$ for all $P \in E$.*
3. *Existence of Inverses: Given P on E, then there exists P' such that $P + P' = \infty$. This is usually denoted $-P$.*
4. *Associativity: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all P_1, P_2, P_3 on E.*

The points on E form an additive abelian group with ∞ as the identity element.

Proof. Commutativity is easy to see geometrically. The line that connects P_1 and P_2 is the same as the line that connects P_2 and P_1. Also, the formulas will show that commutativity holds.

The point at ∞ is the identity by definition.

Since $P = (x, y)$ lies on E, then there is a reflection P' of P across the x-axis where $P' = (x, -y)$. Then $P + P' = \infty$ since $x - x = 0$ and the line connecting P and P' is vertical.

Concerning associativity, consider the case of $A = (x_A, y_A)$, $B = (x_B, y_B)$, $C = (x_C, y_C)$ and $A \neq B \neq C$.

Let $A + B = (x_{A+B}, y_{A+B})$. Let α be slope m_{A+B}

$$\alpha = m_{A+B} = \frac{y_B - y_A}{x_B - x_A}.$$

Then

$$x_{A+B} = \alpha^2 - x_A - x_B$$

and

$$\begin{aligned} y_{A+B} &= \alpha(x_A - x_{A+B}) - y_A \\ &= \alpha(x_A - (\alpha^2 - x_A - x_B)) - y_A \\ &= \alpha(2x_A + x_B - \alpha^2) - y_A. \end{aligned}$$

Let β be slope $m_{(A+B)+C}$:

$$\begin{aligned} \beta &= m_{(A+B)+C} \\ &= \frac{y_C - y_{A+B}}{x_C - x_{A+B}} \\ &= \frac{y_C - [\alpha(2x_A + x_B - \alpha^2) - y_A]}{x_C - (\alpha^2 - x_A - x_B)} \\ &= \frac{y_C + y_A - \alpha(2x_A + x_B - \alpha^2)}{x_A + x_B + x_C - \alpha^2} \end{aligned}$$

Then

$$\begin{aligned} x_{(A+B)+C} &= \beta^2 - x_{A+B} - x_C \\ &= \beta^2 - (\alpha^2 - x_A - x_B) - x_C \\ &= \beta^2 + x_A + x_B - x_C - \alpha^2, \end{aligned}$$

and

$$\begin{aligned}
y_{(A+B)+C} &= \beta(x_{A+B} - x_{(A+B)+C}) - y_{A+B} \\
&= \beta[\alpha^2 - x_A - x_B - (\beta^2 + x_A + x_B - x_C - \alpha^2)] + \beta(x_C - x_{A+B}) - y_C \\
&= \beta(\alpha^2 - x_A - x_B - (\beta^2 + x_A + x_B - x_C - \alpha^2) + x_C - (\alpha^2 - x_A - x_B)) - y_C \\
&= -y_C + \beta(2x_C - x_A - x_B - \beta^2 + \alpha^2).
\end{aligned}$$

Let $\alpha = \alpha_N/\alpha_D$ and let $\beta = \beta_N/\beta_D$ so that

$$\begin{aligned}
\alpha_N &= y_B - y_A \\
\alpha_D &= x_B - x_A \\
\beta_N &= (y_A + y_C)\alpha_D^3 - \alpha_N[(2x_A + x_B)\alpha_D^2 - \alpha_N^2] \\
\beta_D &= (x_A + x_B + x_C)\alpha_D^2 - \alpha_N^2
\end{aligned}$$

Likewise we want to construct the point $A + (B + C) = (x_{A+(B+C)}, y_{A+(B+C)})$. Let $\gamma = m_{B+C}$

$$\gamma = m_{B+C} = \frac{y_B - y_C}{x_B - x_C}.$$

Then

$$x_{B+C} = \gamma^2 - x_B - x_C$$

and

$$\begin{aligned}
y_{B+C} &= \gamma(x_B - x_{B+C}) - y_B \\
&= \gamma(x_B - (\gamma^2 - x_B - x_C) - y_B \\
&= \gamma(2x_B + x_C - \gamma^2) - y_B.
\end{aligned}$$

Let τ be slope $m_{A+(B+C)}$:

$$\begin{aligned}
\tau &= m_{A+(B+C)} \\
&= \frac{y_{B+C} - y_A}{x_{B+C} - x_A} \\
&= \frac{\gamma(2x_B + x_C - \gamma^2) - y_B - y_A}{\gamma^2 - x_B - x_C - x_A} \\
&= \frac{y_A + y_B - \gamma(2x_B + x_C - \gamma^2)}{x_A + x_B + x_C - \gamma^2}
\end{aligned}$$

Then

$$\begin{aligned}
x_{A+(B+C)} &= \tau^2 - x_A - x_{B+C} \\
&= \tau^2 - x_A - (\gamma^2 - x_B - x_C) \\
&= \tau^2 + x_B + x_C - x_A - \gamma^2
\end{aligned}$$

and

$$\begin{aligned}
y_{A+(B+C)} &= \tau(x_A - x_{A+(B+C)}) - y_A \\
&= \tau[x_A - (\tau^2 + x_B + x_C - x_A\gamma^2)] - y_A \\
&= \tau(2x_A - x_B - x_C - \tau^2 + \gamma^2) - y_A.
\end{aligned}$$

Let $\gamma = \gamma_N/\gamma_D$ and $\tau = \tau_N/\tau_D$ so that

$$\begin{aligned}
\gamma_N &= y_B - y_C \\
\gamma_D &= x_B - x_C \\
\tau_N &= (y_A + y_B)\gamma_D^3 - \gamma_N[(2x_B + x_C)\gamma_D^2 - \gamma_N^2] \\
\tau_D &= (x_A + x_B + x_C)\gamma_D^2 - \gamma_N^2
\end{aligned}$$

It can be shown that by multiplying both sides by $\alpha_D^6\gamma_D^6$ to clear denominators in $\beta^2\tau^2$,

$$\begin{aligned}
x_{(A+B)+C} - x_{A+(B+C)} &= \beta^2 + x_A + x_B - x_C - \alpha^2 - (\tau^2 + x_B + x_C - x_A - \gamma^2) \\
&= \beta^2 - \tau^2 + 2x_A - 2x_C + \gamma^2 - \alpha^2 \\
&= \beta_N^2\tau_D^2\gamma_D^2 - \tau_N^2\beta_D^2\alpha_D^2 + [(2x_A - 2x_C)\alpha_D^2\gamma_D^2 + \gamma_N^2\alpha_D^2 - \alpha_N^2\gamma_D^2]\beta_D^2\tau_D^2 \\
&= 0.
\end{aligned}$$

It can be shown that multiplying both sides by $\alpha_D^9\gamma_D^9$ to clear denominators in $\beta^3\tau^3$,

$$\begin{aligned}
y_{(A+B)+C} - y_{A+(B+C)} &= (y_A - y_C) + \beta(2x_C - x_A - x_B - \beta^2 + \alpha^2) \\
&\quad -\tau(2x_A - x_B - x_C - \tau^2 + \gamma^2) \\
&= (y_A - y_C)\beta_D^3\tau_D^3\alpha_D^3\gamma_D^3 \\
&\quad +\beta_N\tau_D^3\gamma_D^9[(2x_C - x_A - x_B)\beta_D^2\alpha_D^2 - \beta_N^2 + \alpha_N^2\beta_D^2] \\
&\quad -\tau_N\beta_D^3\alpha_D^9[(2x_A - x_B - x_C)\tau_D^2\gamma_D^2 - \tau_N^2 + \gamma_N^2\tau_D^2] \\
&= 0.
\end{aligned}$$

The other cases can be done similarly. The case above is solely the case of 2D of the algorithm of adding points listed above, and one can see that the calculations are long and arduous. It suffices to say that proof of associativity is tedious. Geometrically, the proof can be easy to see.

Associativity can be done by using explicit equations or by using homogeneous equations. We leave this to Washington [20]. □

4.5. Theorems on Group Structure

The question of the structure of the group on an elliptic curve was first posed by Henri Poincaré in 1901. The first proof came from Louis Mordell in 1922 and taken up again by André Weil in 1928.

Theorem 4.5.1 (Mordell-Weil Theorem). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Theorem 4.5.2 (Fundamental Theorem of Finitely Generated Abelian Groups). *Let A be a finitely generated abelian group. Then*

$$A \cong \mathbb{Z}^r \times B$$

*where B is some finite abelian group. For a given abelian group A, the isomorphism above is unique, thus r is unique and r is call the **rank** of A.*

Concerning elliptic curves, the rank r is the number of independent basis points that have infinite order. The rank of a curve is not easily calculated. There is no known method for finding those independent basis points. It is not known if r can be arbitrarily large. The largest known rank is at least 28 found in 2006 which is given by

$$y^2 + xy + y = x^3 - x^2$$

$$-20\,067\,762\,415\,575\,526\,585\,033\,208\,209\,338\,542\,750\,930\,230\,312\,178\,956\,502x$$

$$+34\,481\,611\,795\,030\,556\,467\,032\,985\,690\,390\,720\,374\,855$$

$$944\,359\,319\,180\,361\,266\,008\,296\,291\,939\,448\,732\,243\,429$$

where the last two lines represent 1 83-digit decimal number. This was discovered by Noam Elkies in 2006 [6]. The question of the nature of r is the Birch and Swinnerton-Dyer conjecture, which is one of the seven Millenial problems. Just as we have looked at the group of points of an elliptic curve E over the rationals, the group $E(\mathbb{Q})$, we can consider E over other fields $\mathbb{F}_p$ for prime p. These groups are simply noted $E(\mathbb{F}_p)$.

For the Hasse-Weil L function at $s = 1$,

$$L(E, 1) = \prod_p (1 - 2a_p p^{-s} + p^{1-2s})^{-1}$$

where a_p is determined from $\#E(\mathbb{F}_p) = p + 1 - a_p$ for each p.

Conjecture 4.5.3 (Birch-Swinnerton-Dyer Weak Form)**.** *$L(E, 1) = 0 \iff E$ has infinitely many rational points.*

The strong version of the conjecture states the relation between the rank r of a curve C in the projective plane and the L function.

Points P whose order is finite are called **torsion points.** These torsion points are a subgroup of $E(\mathbb{Q})$. The following theorem allows for a quick determination of the number of torsion points of the group over $\mathbb{Q}$.

Theorem 4.5.4 (Lutz-Nagell Theorem)**.** *Let E be defined by $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$. Let $P = (x, y) \in E(\mathbb{Q})$ with $ord(P) < \infty$. Then $x,\ y \in \mathbb{Z}$. If $y \neq 0$, then*

$$y^2 \mid 4A^3 + 27B^2.$$

The Lutz-Nagell theorem ([20] p.195) gives a bound on the size of the torsion group in terms of the curve's discriminant. Although it is unclear whether rank is unbounded, the number of possible groups of torsion points is limited to the 15 groups listed below in Mazur's theorem.

Theorem 4.5.5 (Mazur)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup of $E(\mathbb{Q})$ is one of the following:*

$$\mathbb{Z}_n \text{ with } 1 \leq n \leq 10 \text{ or } n = 12$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \text{ with } 1 \leq n \leq 4.$$

Now we state Hasse's theorem which puts bounds on the size of a group over a field F of prime q.

Theorem 4.5.6 (Hasse's Theorem)**.** *Let E be defined over a field $\mathbb{F}_q$, for some prime q. Then the order of $E(\mathbb{F}_q)$, denoted $\#E(\mathbb{F}_q)$, satisfies*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

This is equivalent to saying that $E(\mathbb{F}_q)$ falls in the interval $q+1-2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q+1+2\sqrt{q}$, which we will call Hasse's Interval.

5. EXAMPLES

5.1. Examples Over the Rationals

5.1.1. Chord-Tangent Method Continued.

In section 2.4, we looked at

$$y^2 = x^3 + 2 \tag{5.1}$$

over the rationals with $P = (-1, 1)$. Recall that we defined $\star$ as the operation of finding the third point where a line intersects an elliptic curve E. In this case, we saw that when we took the line tangent to the curve at this point, we found that the tangent line intersected the curve at $\left(\frac{17}{4}, \frac{71}{8}\right) = P \star P$. With reflection across the x-axis, then $P + P = \left(\frac{17}{4}, -\frac{71}{8}\right) = 2P$.

The line adjoining P and $2P$ is entirely different from the tangent line at P and will cross E at a third point. We find the slope between the two points is $-79/42$ and the equation of the line through the two points is $y = -\frac{79}{42}x - \frac{37}{42}$. Substitute this into Eq. (5.1) and factor and we find a third x-coordinate of $x = 127/441$. We plug this into Eq. (5.1) and find $y^2 = \frac{173\,580\,625}{85\,766\,121}$ and $y = \pm\frac{13175}{9261}$. Then $P \star 2P = \left(\frac{127}{441}, -\frac{13175}{9261}\right)$ and $P + 2P = \left(\frac{127}{441}, \frac{13175}{9261}\right)$.

Figure 5.1 on right shows E and P from the example, the line tangent to E at P, the operation $P \star P$, and the operation $P + P$. Let $Q = 2P$. The right shows the analogue

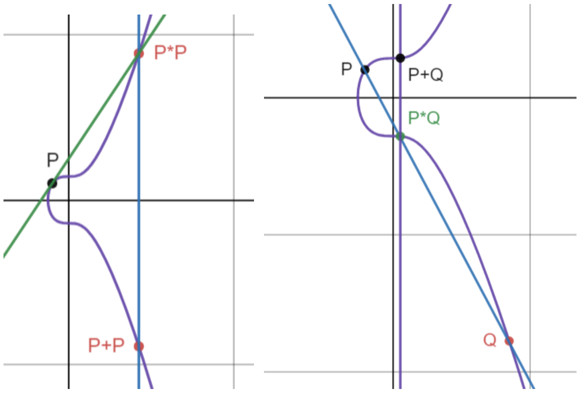


Figure 5.1: Chord-Tangent Method with reflection

for $P + Q$.

5.1.2. Example 1. Consider curve E :

$$y^2 = x^3 + 1. \tag{5.2}$$

We see that that the point $P = (2, 3)$ is a rational point on Eq. (5.2). Say we want to find points $2P$, $3P$, $4P$, etc. First, we take the derivative of Eq. (5.2) with respect to x, and find the slope $m = dy/dx$ at P. We see then that $2y\ dy = 3x^2dx \Rightarrow 6dy = 12dx \Rightarrow m = 2$. Then using slope-intercept form, $3 = 2 \cdot 2 + b$, which shows that the tangent line is

$$y = 2x - 1. \tag{5.3}$$

Now, we substitute Eq. (5.3) into Eq. (5.2) to obtain $(2x - 1)^2 = x^3 + 1$, thus

$$0 = x^3 - 4x^2 - 4x \tag{5.4}$$

We already know that $x = 2$ is a double root of Eq. (5.4) since we took the tangent to E at $x = 2$. Since x factors out of all three terms, $x = 0$ is the 3rd root. Plugging $x = 0$ into Eq. (5.3), we find that $P \star P = (0, -1)$ and $P + P = 2P = (0, 1)$.

To find $3P = P + 2P$, first we find the slope between the two points, which is $m = 1$. Thus the equation of the line connecting P and $2P$ is $y = x + 1$. We substitute this into Eq. (5.2) to find $(x + 1)^2 = x^3 + 1$. Thus,

$$0 \;\; = \;\; x^3 - x^2 - 2x. \tag{5.5}$$

We already know that $x = 2$ and $x = 0$ are roots from P and $2P$ respectively, so we find that $x = -1$ is the 3rd root. Plugging this into $y = x + 1$, we find $y = 0$, and this yields $3P = (-1, 0)$.

We see that $y = 0$ on $(-1, 0)$, so $3P$ has order 2, thus P has order 6. Figure 5.2 shows the curve and the addition of points.

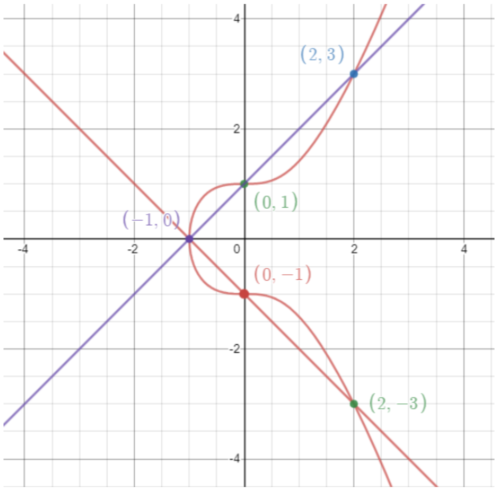


Figure 5.2: $y^2 = x^3 + 1$

5.1.3. Example 2. Consider the curve

$$x^3 + y^3 + 1 = 5xy \tag{5.6}$$

Let's say that we want to find rational solutions to this curve. We can use the addition law to find those points. Note that in this example, we will be using $y = x$ as the line of reflection, rather than reflecting across $x = 0$. Upon inspection we see that (2,1) is a solution, so $P = (2, 1)$.

We can then find tangent lines, points of intersection and use reflection to find those points. Taking the derivative, then $3x^2 + 3y^2y' = 5y + 5xy'$. Plugging in $(2, 1)$, then $y' = 1$. The equation of tangent line is $y = x - 1$.

Plugging this into Eq. (5.6);

$$\begin{aligned} x^3 + (x-1)^3 + 1 &= 5x(x-1) \\ x^3 + x^3 - 3x^2 \cdots &= 5x^2 - 5x \\ 0 &= 2x^3 - 8x^2 + \cdots \\ &= x^3 - 4x^2 + \cdots \end{aligned}$$

The sum of the roots add up to the opposite of the x^2 term after dividing by the leading coefficient, thus $x_3 = 4 - 2 - 2 = 0$. This yields the point $(0, -1)$. Reflected across the line $y = x$, we have $2P = (-1, 0)$.

For $3P = P + 2P$, finding the slope and the y-intercept, the equation between the two points is $y = \frac{1}{3}x + \frac{1}{3}$.

Plug this into Eq. (5.6)

$$\begin{aligned} x^3 + \left(\frac{1}{3}x + \frac{1}{3}\right)^3 + 1 &= 5x\left(\frac{1}{3}x + \frac{1}{3}\right) \qquad (5.7) \\ x^3 + \frac{1}{27}x^3 + \frac{1}{9}x^2 + \cdots &= \frac{5}{3}x^2 + \frac{5}{3}x \\ 0 &= \frac{28}{27}x^3 - \frac{14}{9}x^2 + \cdots \\ &= x^3 - \frac{3}{2}x^2 + \cdots . \end{aligned}$$

We take the opposite of x^2 term and subtract the two known roots. Then $x_3 = 3/2 - -1 - 2 = 1/2$. Finding y, and reflecting across $y = x$, then $3P = \left(\frac{1}{2}, \frac{1}{2}\right)$.

To find $4P = P + 3P$, we find the equation between the 2 lines and see that $y = \frac{1}{3}x + \frac{1}{3}$. This leads us to the substitution in Eq. (5.7), so we subtract out the known roots. Then $x_3 = 3/2 - 2 - 1/2 = -1$. We find then that $y = 0$. We reflect across $y = x$, so that $4P = (0, -1)$.

To find $5P = P + 4P$, we find the equation between the two points, $y = x - 1$. This leads to the substitution in Eq. (5.6). We subtract the known roots, which is $x_3 = 4 - 2 - 0 = 2$. We find $y = 1$. Reflect across $y = x$, we find $5P = (1, 2)$.

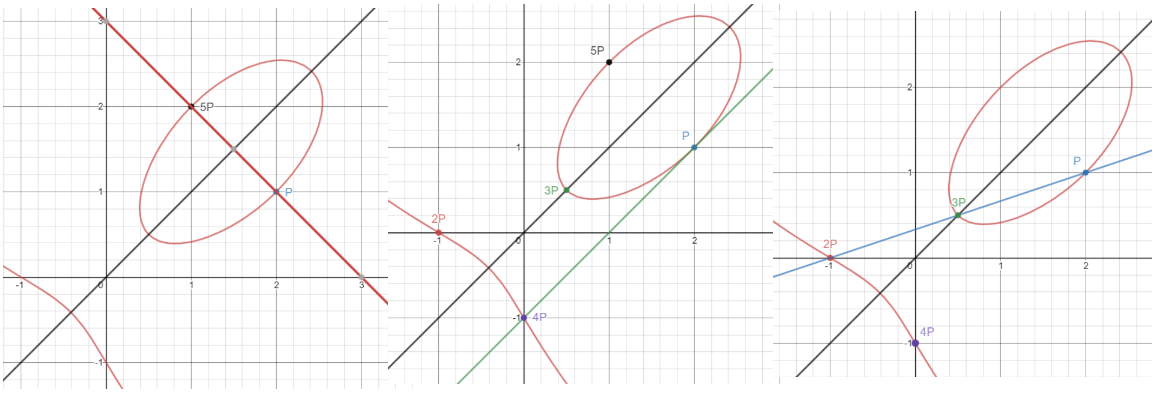
We find the slope between the two points, $m = -1$. This slope is perpendicular to our line of reflection, so this gives us the point at infinity, so $6P = \infty$.

Therefore $(2, 1)$ has order 6. It turns out then that this elliptic curve contains only a finite number of rational points. Figure 5.3 shows the different multiples kP up to $6P = \infty$.

5.1.4. Example 3.

Consider the problem of finding integer solutions to

$$a^3 + b^3 + c^3 = 6abc. \qquad (5.8)$$



(a) P=(2,1)
6P $= \infty$

(b) 2P=(-1,0);
5P $=$ (1,2)

(c) 3P=(1/2,1/2);
4P=(0,-1)

Figure 5.3: $x^3 + y^3 + 1 = 5xy$

Suppose that we want to know rational roots to Eq. (5.8). Upon inspection, we see that $(1, 2, 3)$ is a solution to Eq. (5.8). The permutations $(2, 1, 3)$ $(3, 1, 2)$, $(1, 3, 2)$, $(2, 3, 1)$, and $(3, 2, 1)$ are also solutions to Eq. (5.8). We can ask if there is a finite or an infinite number of primitive solutions (i.e. solutions with no common factor). We can use elliptic curves and the addition group law to find the answer to these questions.

First, let's dehomogenize by dividing by c^3. Then, define new variables $x = \frac{a}{c}$ and $y = \frac{b}{c}$. to get

$$x^3 + y^3 + 1 = 6xy \tag{5.9}$$

Since we have divided by c, then the following are all solutions of Eq. (5.9):

$$\left(\tfrac{1}{3}, \tfrac{2}{3}\right) \quad \left(\tfrac{2}{3}, \tfrac{1}{3}\right) \quad \left(\tfrac{3}{2}, \tfrac{1}{2}\right) \quad \left(\tfrac{1}{2}, \tfrac{3}{2}\right) \quad (2, 3) \quad (3, 2) \ .$$

It also turns out that $(-1, 0)$ and $(0, -1)$ are solutions to Eq. (5.9).

We want to double a point and see if it leads to a new set of solutions. Applying implicit differentiation to Eq. (5.9) at the point $(2, 3)$, we find that $y' = \frac{6y-3x^2}{3y^2-6x}$, and $y'(P) = \frac{2}{5}$. The equation of the line through $(2, 3)$ is given by

$$y = \frac{2}{5}x + \frac{11}{5}. \tag{5.10}$$

Substitute Eq. (5.10) into Eq. (5.9)

$$\begin{aligned} x^3+\left(\frac{2}{5}x+\frac{11}{5}\right)^3 &= 6x\left(\frac{2}{5}x+\frac{11}{5}\right) \\ x^3+\frac{8}{25}x^3+\frac{132}{125}x^2+\cdots &= \frac{12}{5}x^2 \\ \frac{133}{125}x^3-\frac{168}{125}x^2+\cdots &= \cdots\,. \end{aligned} \tag{5.11}$$

Divide Eq. (5.11) by 133/125 and the coefficient of the x^2 term is $-24/19$. We find the 3rd root by subtracting the double known root from the opposite of the coefficient, $x_3 = 24/19 - 2 - 2 = -52/19$. Plug this into Eq. (5.10) to obtain y_2, reflect across $y = x$ and we find $2P = \left(\frac{21}{19}, \frac{-52}{19}\right)$.

Let's reconsider Eq. (5.9) to obtain a new triplet solution to Eq. (5.8). Since $x = a/c$ and $y = b/c$ in Eq. (5.9), when we multiply by c (i.e. when we homogenize), we obtain 3 integers. Therefore $(19, 21, -52)$ is a primitive solution of Eq. (5.8). We can take the permutations and divide by c to obtain a new family of solutions to Eq. (5.9).

$$\left(-\tfrac{19}{52},-\tfrac{21}{52}\right)\quad\left(-\tfrac{21}{52},-\tfrac{19}{52}\right)\quad\left(-\tfrac{52}{21},\tfrac{19}{21}\right)\quad\left(\tfrac{19}{21},-\tfrac{52}{21}\right)\quad\left(\tfrac{21}{19},-\tfrac{52}{19}\right)\quad\left(-\tfrac{52}{19},\tfrac{21}{19}\right)\ .$$

We can continue to find more and more families of solutions: $P + 2P = (2, 3) + (21/19, -52/19) = (1817/3258, 5275/3278)$. Thus (1817, 3258, 5275) is another solution to Eq. (5.8), which will then create a new family of solutions to Eq. (5.9). Continuing in this manner, we can find infinitely many families of solutions to Eq. (5.8).

Figure 5.4 shows the first two families of rational points on the curve discussed above.

5.1.5. Example 4.

Consider the curve

$$y^2 = x^3 + 3x. \tag{5.12}$$

We see that $P = (1, 2)$ is a rational solution of Eq. (5.12). For this example we will find points $2P$, $3P$, and $4P$. We notice that this equation is in Weierstrass normal form, so we can use the shortcuts of the methods listed in § 4.3 to find k-multiples of P, rather

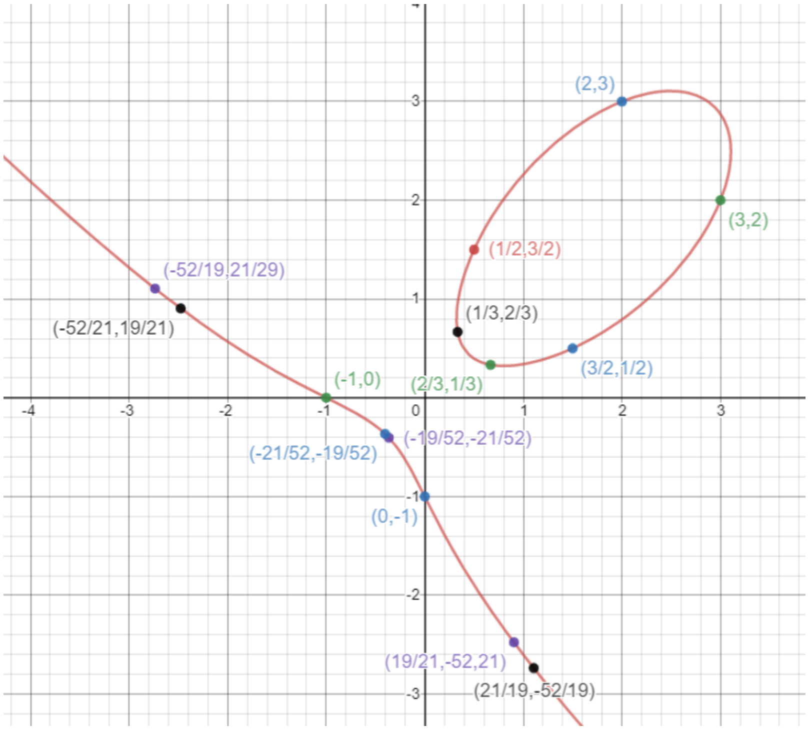


Figure 5.4: $x^3 + y^3 + 1 = 6xy$

than using the method of substitution that was used in the three examples above.

To find $2P = P + P$, we find the slope of the line that is tangent to Eq. (5.12) through the point $(1, 2)$. We see that when we differentiate with respect to x and evaluate at $(1, 2)$, then $dy/dx = (3x^2 + 3)/(2y) = 3/2$. Since we took the tangent, then $x = 1$ is a double root, and we find $x_3 = m^2 - x_1 - x_2 = (3/2)^2 - 1 - 1 = 1/4$ as a 3rd root. We find that $y_3 = m(x_1 - x_3) - y_1 = \frac{3}{2}\left(1 - \frac{1}{4}\right) - 2 = -\frac{7}{8}$. Thus $2P = \left(\frac{1}{4}, -\frac{7}{8}\right)$.

To find $3P = P + 2P$, we will take the slope between $(1, 2)$ and $\left(\frac{1}{4}, -\frac{7}{8}\right)$, and we find that $m = 23/6$. We know that $x = 1$ and $x = 1/4$ are roots, thus we find $x_3 = m^2 - x_1 - x_3 = \frac{529}{36} - 1 - \frac{1}{4} = 121/9$. We find $y_3 = m(x_1 - x_3) - y_1 = \frac{23}{6}\left(1 - \frac{121}{9}\right) - 2 = \frac{-1342}{27}$. Thus, $3P = \left(\frac{121}{9}, \frac{-1342}{27}\right)$.

To find $4P = P + 3P$, we find the slope of the line between the points $(1, 2)$ and $\left(\frac{121}{9}, \frac{-1342}{27}\right)$. We find then that $m = -\frac{349}{84}$. We know that $x = 1$ and $x = 121/9$ are roots, and we find that $x_3 = m^2 - x_1 - x_3 = \frac{121801}{7056} - 1 - \frac{121}{9} = \frac{2209}{784}$. We find $y_3 = m(x_1 - x_3) - y_1 = -\frac{349}{84}\left(1 - \frac{2209}{784}\right) - 2 = \frac{121871}{21952}$. Thus, $4P = \left(\frac{2209}{784}, \frac{121871}{21952}\right)$.

Upon further investigation, we find

$$5P = \left(\frac{26\ 499}{35\ 678\ 000}, -\frac{22\ 304\ 640\ 511}{470\ 527\ 400\ 000}\right),$$

and we can see that rational points, even after just a few iterations, can become quite unwieldly.

5.2. An Example Over a Finite Field

Examining elliptic curves over most fields does not make sense geometrically. So, to conceptualize we have begun by constructing elliptic curves over the reals and examining their graphs. We now consider elliptic curves over different fields. Let's again consider the curve

$$y^2 = x^3 + 3x \pmod 5. \tag{5.13}$$

This time, we are considering the curve over $\mathbb{F}_5$, the field of 5 elements. Maybe not surprisingly, we can still use the methods outlined in § 4.3 to find the addition of points. Here, we still have that $P = (1, 2)$ is a solution of Eq. (5.13). We want to find points $2P$, $3P$, and $4P$.

To find $2P$, we want to find the slope of the line tangent to the curve, so taking the derivative with respect to x and evaluating at $(1, 2)$, we see $2y\ dy = (3x^2 + 3)dx \Rightarrow 4dy = 6dx$. Since we are now operating modulo 5 instead of over the rationals, as noted above, division corresponds to multiplying by the multiplicative inverse. We immediately see that $4^{-1} \equiv 4 \pmod 5$, thus we multiply both sides by 4, and find $dy/dx = 6 \cdot 4 = 24 \equiv 4 \pmod 5$. The slope of the tangent line is $m = 4$ we can find the 3rd x root just as we did in the algorithm of § 4.3. Thus, given that $x_1 = x_2 = 1$, then $x_3 = m^2 - 2x_1 = 16 - 2 = 14 \equiv 4 \pmod 5$. We find $y_3 = m(x_1 - x_3) - y_1 = 4(1 - 4) - 2 = -14 \equiv 1$. Thus, $2P = (4, 1)$.

To find $3P = P + 2P$, we take the slope between the two points. Since we are mod

5, it is helpful to think of slope as $m = (y_2 - y_1)(x_2 - x_1)^{-1}$. The slope between $(1, 2)$ and $(4, 1)$ is $m = (1 - 2)(4 - 1)^{-1} = 4 \cdot 2 = 8 \equiv 3 \pmod 5$. We find $x_3 = m^2 - x_1 - x_2 = 3^2 - 1 - 4 = 4 \pmod 5$. We find that $y_3 = m(x_1 - x_3) - y_1 = 3(1 - 4) - 2 = -11 \equiv 4 \pmod 5$. Thus, $3P = (4, 4)$.

To find $4P = P + 3P$, we find the slope between $(1, 2)$ and $(4, 4)$ by $m = (4-2)(4-1)^{-1} = 2 \cdot 2 \equiv 4 \pmod 5$. Then we find $x_3 = 4^2 - 1 - 4 \equiv 1 \pmod 5$. Also, we see that $y_3 = 4(1 - 1) - 2 \equiv 3 \pmod 5$. Thus, $4P = (1, 3)$.

To find $5P = P + 4P$, we want to find that the slope between the points $P = (1, 2)$ and $4P = (1, 3)$. It is easy to see that the slope between these two points is undefined, thus $5P$ brings us to the identity, the point where all vertical lines intersect, thus $5P = \infty$.

Let $\mathcal{O}(P)$ denote the order of a point P, that is, $\mathcal{O}(P) = \min\{n | nP = \infty\}$. Thus, we see that $(1, 2)$ has order 5, or $\mathcal{O}(1, 2) = 5$.

Upon further investigation, we find other rational points that hold for Eq. (5.13) and their corresponding orders.

$$\begin{array}{ccccc} O(2,2) = 10 & O(1,2) = 5 & O(0,0) = 2 & O(2,3) = 10 & O(1,3) = 5 \\ O(\infty) = 1 & O(3,1) = 10 & O(4,1) = 5 & O(3,4) = 10 & O(4,4) = 5 \end{array}$$

We have already mentioned that the addition of points follows group laws and have shown that group axioms hold for point addition. In this example, since we let our curve be modulus 5, we see that Eq. (5.13) generates a group of 10 elements that are indeed congruent to $\mathbb{Z}_{10}$, an additive abelian group.

Let's reconsider the normalized Weierstrass form mod 5:

$$y^2 = x^3 + Ax + B.$$

Firstly, since we are using modulus 5, there are 25 elliptic curves to consider (since $A \in \{0, 1, 2, 3, 4\}$ and $B \in \{0, 1, 2, 3, 4\}$. Are all the groups induced by changing A and B the same? In fact, they are not. Table 5.1 shows what group $E(\mathbb{F}_5)$ is isomorphic to for the given A and B. Entries with an X in the table indicate that for the chosen A and B,

Table 5.1: Group Isomorphisms

	B=0	B=1	B=2	B=3	B=4
A=0	X	$\mathbb{Z}_6$	$\mathbb{Z}_6$	$\mathbb{Z}_6$	$\mathbb{Z}_6$
A=1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_9$	$\mathbb{Z}_4$	$\mathbb{Z}_4$	$\mathbb{Z}_9$
A=2	$\mathbb{Z}_2$	$\mathbb{Z}_7$	X	X	$\mathbb{Z}_7$
A=3	$\mathbb{Z}_{10}$	X	$\mathbb{Z}_5$	$\mathbb{Z}_5$	X
A=4	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\mathbb{Z}_8$	$\mathbb{Z}_3$	$\mathbb{Z}_3$	$\mathbb{Z}_8$

the quantity $4A^3 + 27B^2 \equiv 0 \pmod 5$, thus the curve is not of Weierstrass form and no group exists.

5.3. Finding the Order of a Group

Previously, we mentioned that the order of the group $E(\mathbb{F}_q)$ of an elliptic curve E fell into what is called Hasse's Interval, $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$. Finding the exact order of such a group or finding the order of a particular point $P \in E(\mathbb{F}_q)$ is easy. There are methods and processes for finding the orders of these.

5.3.1. Baby Step-Giant Step. Below, the Baby Step-Giant Step (BSGS) algorithm is outlined in Washington ([20] § 4.3.4) and an example is provided. Given point $P \in E(\mathbb{F}_q)$, q a prime power, we wish to find the order of P.

First, let $Q = (q + 1)P$. Choose an integer $m > q^{1/4}$. Compute jP for $0, 1, 2, \ldots, m$. Calculate $Q + k(2m)P$ for integers $k = [-m, \ldots, m]$. Look for a match in the x-coordinates in the small jumps of jP and the large jumps of $Q + 2kmP$. For a matching x-coordinate, conclude that if the y-coordinates also match, then $Q + 2kmP = jP$, otherwise, conclude that $Q + 2kmP = -jP$. Thus $(q + 1 + 2km \mp j)P = \infty$. Let $M = q + 1 + 2mk \mp j$ and conclude M is a multiple of the order of P. Determine the primes $p_1, p_2, \ldots, p_l$ that divide M. Test $(M/p_i z)P$. If $(M/p_i)P = \infty$, then M/p_i is a new candidate for the order of P

and substitute $M/p_i \to M$. Continue testing each $p_i|M$ for $(M/p_i)P = \infty$ and divide out the p_i that induce the identity. If $(M/p_i)P \neq \infty$ for each p_i, then conclude M is the order of P.

To find the order of the group, it may be possible to tell the order of the group from the known order of one point. By Lagrange's Theorem, for N such that $N = \#E(\mathbb{F}_q)$, then $NP = \infty$ for all $P \in E(\mathbb{F}_q)$. Then $N = kM$ for some k-multiple of M. By Hasse's Theorem, we know $q+1-2\sqrt{q} \leq N = kM \leq q+1-2\sqrt{2}$. Then, if the following inequality holds for some k-multiple of M,

$$(k-1)M < q+1-2\sqrt{q} \leq kM \leq q+1+2\sqrt{q} < (k+1)M,$$

then we can conclude that $kM = \#E(\mathbb{F}_q)$ is indeed the order of the group.

If it is not possible to establish the order of the group using the known order M of one point P, then it will be necessary to find the order of several other random points of E. Find orders of those points until the greatest common multiple of these orders divides only one number N such that $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. Then conclude $N = \#E(\mathbb{F}_q)$.

Lastly, we wish to note that BSGS is useful since the number of integers to be tested to find a multiple of the order of P from $(q+1+2\sqrt{q})-(q+1-2\sqrt{q}) = 4\sqrt{q}$ is taken down to $4\sqrt[4]{q}$ steps.

5.3.2. Example. Determine the order of the group induced by E such that

$$y^2 = x^3 + 3x - 13 \pmod{331}.$$

The reader can verify that $P = (2,1)$ satisfies E. Since $q = 331$, compute $Q = (q+1)P = 332P = (247, 50)$. Since $q^{1/4} \approx 4.27$, chose $m = 5$. Table 5.2 shows j-multiples of P from $-m = -5$ to $m = 5$. Since $m = 5$, Table 5.3 shows $(q+1+2mk)P$-multiples for integers $k = -5, ..., 5$.

Notice then that $Q + 0 \cdot 10P = 332P \equiv -3P \pmod{331}$. We conclude then that $Q + 3P = \infty$ and let $M = q + 1 + 3 = 331 + 1 + 3 = 335$ be a multiple of order of P.

Table 5.2: Baby Steps for Determining Point Order

jP	jP
$0P = \infty$	
$P = (2, 1)$	$-P = (2, 330)$
$2P = (135, 160)$	$-2P = (135, 171)$
$3P = (247, 281)$	$-3P = (247, 50)$
$4P = (9, 322)$	$-4P = (9, 9)$
$5P = (268, 48)$	$-5P = (268, 283)$

Table 5.3: Giant Steps for Determining Point Order

$(q + 1 + 2mk)P$	$(q + 1 + 2mk)P$
$282P = (7, 196)$	$292P = (31, 322)$
$302P = (143, 30)$	$312P = (32, 197)$
$322P = (84, 303)$	$332P = (247, 50)$
$342P = (91, 12)$	$352P = (50, 130)$
$362P = (191, 259)$	$372P = (253, 67)$
$382P = (40, 104)$	

Factoring M finds that $M = 5 \cdot 67$. For $p_i = 5$, we see that

$$(M/p_i)P = 67P = (280, 307) \neq \infty.$$

For $p_i = 67$, then

$$(M/p_i) = 5P = (268, 48) \neq \infty.$$

Since $(M/p_i)P \neq \infty$ for all $p_i|M$, we then can conclude that $M = 335$ is the order of P.

To find the order of the group, let us first consider M. We know from Hasse's Theorem that $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$. Since $q = 331$ and $\sqrt{q} \sim 36.4$, then

$$296 \leq \#E(\mathbb{F}_q) \leq 368$$

Consider that $M = 335$, we can easily see that $1 \cdot 335$ is the only multiple of 335 that fits in the Hasse Interval. Thus we conclude that $\#E(F_{331}) = 335$.

5.4. Applications

5.4.1. The Hardy-Ramanujan Problem. The story goes that G. H. Hardy went to go visit Srinivasa Ramanujan in the hospital. On his way to the hospital he had ridden in taxicab number 1729, which he remarked to Ramanujan that it seemed "a rather dull" number, to which Ramanujan remarked, "No, it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways." Hardy followed up the remark by asking Ramanujan, what number was the smallest number that could be written as the sum of 4th powers in two different ways? To this, Ramanujan replied that he did not know [27], [19].

We can use the method of looking for rational points on a cubic to answer this question.

Let's reformulate the question into four unknown integers:

$$a^4 + b^4 = c^4 + d^4. \tag{5.14}$$

Dehomgenizing (5.14) by dividing by c^4, we choose new variables x, y, and z, such that $x = \frac{a}{c}$, $y = \frac{b}{c}$, and $z = \frac{d}{c}$ to obtain a surface S defined by

$$x^4 + y^4 = z^4 + 1. \tag{5.15}$$

Choose a parameter t. The line ℓ_1 whose equation is given by

$$(x, y, z) = (t, 1, t) \tag{5.16}$$

satisfies Eq. (5.15) and lies on S. For any given constant λ, the plane Π whose equation is given by

$$\lambda x + y - \lambda z - 1 = 0 \quad \text{or} \quad y = -\lambda x + \lambda z + 1 \tag{5.17}$$

contains ℓ_1. Since ℓ_1 lies on S and Π contains ℓ_1, then the intersection of S and Π will give a 4^{th} degree curve that contains a line. In other words, the 4^{th} degree polynomial curve must factor into a linear and a cubic. Substituting the expression for y in Eq. (5.17) into Eq. (5.15) gives

$$x^4 + (-\lambda x + \lambda z + 1)^4 = z^4 + 1$$

which can be factored into $(x - z)h_\lambda(x, z) = 0$ where

$$\begin{aligned} h_\lambda(x,z) &= -4\lambda + 6\lambda^2 x - 4\lambda^3 x^2 + x^3 + \lambda^4 x^3 - 6\lambda^2 z + 8\lambda^3 xz + x^2 z \\ &\quad -3\lambda^4 x^2 z - 4\lambda^3 z^2 + xz^2 + 3\lambda^4 xz^2 + z^3 - \lambda^4 z^3. \end{aligned} \tag{5.18}$$

We want to use our elliptic curve techniques on the elliptic curve defined by Eq. (5.18). In order to do so, we need to have a point with rational coordinates on the curve. We will see where the line $(t, 1, t)$ meets the curve. Since $x = t$ and $z = t$, let $x = z$ so that $h_\lambda(x, z) = h_\lambda(x, x) = 0$. This simplifies Eq. (5.18) to $0 = -4\lambda + 4x^3$. Therefore, $x^3 = \lambda$.

Since we are only interested in rational (eventually solely integer) solutions to Eq. (5.15), we let $p = \sqrt[3]{\lambda}$ for some $p \in \mathbb{Q}$. Then $\lambda = p^3$ and Eq. (5.18) becomes

$$\begin{aligned} h_2(x,z) &= -4p^3 + 6p^6 x - 4p^9 x^2 + x^3 + p^{12} x^3 - 6p^6 z + 8p^9 xz + x^2 z \\ &\quad -3p^{12} x^2 z - 4p^9 z^2 + xz^2 + 3p^{12} xz^2 + z^3 - p^{12} z^3. \end{aligned} \tag{5.19}$$

Since $x^3 = \lambda = p^3$ by construction, then $x = p$. Since the point of intersection (x, z) between the line $(t, 1, t)$ and Eq. (5.18) occurred when $x = z$, then we let $P = (x, z) = (p, p)$ be a point of rational coordinates satisfying the cubic polynomial h_2.

Here, we could try find $2P$ using the methods of point addition, by taking the tangent line and finding a third point. This method yields nothing of use, so it become necessary to look for a different point on our curve with rational coordinates.

Consider the line ℓ_2 given by the equation

$$(x,y,z) = (1,t,-t) \tag{5.20}$$

that also satisfies Eq. (5.15) and lies on S. Since the intersection of Π and S produces a line and a cubic, then the intersection of Π and ℓ_2 must either be on the line ℓ_1 or the cubic h_2. It is clear that ℓ_2 and ℓ_1 do not intersect. Thus the intersection of Π and ℓ_2 must be a second point of cubic h_2.

Therefore, we want to know where plane Π and l_2 intersect. We do so by substituting Eq. (5.20) into Eq. (5.17). Then $\lambda + t + \lambda t - 1 = 0$ and $t = \frac{1-p^3}{1+p^3}$. Given the parameters of ℓ_2, where $x = 1$, and $z = -t$, now we have point $Q = (x,z) = \left(1, \frac{p^3-1}{1+p^3}\right)$, a second point with rational coordinates that also satisfies the cubic h.

Now we can consider a new line l_3 that goes through P and Q and we can find where it intersects h_2 a third time. A straightforward computation shows that ℓ_3 is given by the equation

$$z = \frac{1+p-p^3+p^4}{(1-p)(1+p^3)}x + \frac{2p}{(1-p)(1+p^3)} \tag{5.21}$$

Substitute Eq. (5.21) into Eq. (5.19) and find

$$-\frac{4p(p-x)(x-1)(p+3p^2-2p^3+p^5+p^7-x-p^2x+2p^4x-3p^5x-p^6x)}{(p-1)^2(1+p)(1-p+p^2)^2} = 0$$

We find linear terms $x = p$ and $x = 1$, as we must. Solving for x in the last linear factor of h_3, we find

$$x \;=\; \frac{p+3p^2-2p^3+p^5+p^7}{1+p^2-2p^4+3p^5+p^6} \tag{5.22}$$

Substitute Eq. (5.22) into Eq. (5.21) to find the z-coordinate.

$$z = \frac{p-3p^2-2p^3+p^5+p^7}{1+p^2-2p^4+3p^5+p^6} \tag{5.23}$$

Find the y-coordinate by substituting Eq. (5.22) and Eq. (5.23) into Eq. (5.18).

$$y = \frac{1+p^2-2p^4-3p^5+p^6}{1+p^2-2p^4+3p^5+p^6} \tag{5.24}$$

We now have a 4-tuple, say $R = (x, y, z, 1)$, that satisfies Eq. (5.15).

$$R = \left(\frac{p+3p^2-2p^3+p^5+p^7}{1+p^2-2p^4+3p^5+p^6}, \frac{1+p^2-2p^4-3p^5+p^6}{1+p^2-2p^4+3p^5+p^6}, \frac{p-3p^2-2p^3+p^5+p^7}{1+p^2-2p^4+3p^5+p^6}, 1\right)$$

Since $p \in \mathbb{Q}$, let $p = m/n$, for $m,\ n \in \mathbb{N}$. The lowest common denominator e of R can be shown to be $e = n(m^6+3m^5n-2m^4n^2+m^2n^4+n^6)$. Since R satisfies Eq. (5.15), R also satisfies Eq. (5.14). Then we can let $R^* = Re = (ex, ey, ez, e) = (a, b, c, d)$. where a, b, c, and d are given by

$$\begin{aligned} a &= mn^6+3m^2n^5-2m^3n^4+m^5n^2+m^7 \\ b &= n^7+m^2n^5-2m^4n^3-3m^5n^2+m^6n \\ c &= mn^6-3m^2n^5-2m^3n^4+m^5n^2+m^7 \\ d &= m^6n+3m^5n^2-2m^4n^3+m^2n^5+n^7. \end{aligned}$$

If we choose $m = 1$, and $n = 1$, we get $(4, -2, -2, 4)$. However, if we choose $m = 2$ and $n = 1$, we get $(158, -59, 134, 133)$ which is equivalent to $(158, 59, 134, 133)$. A simple computer search shows that

$$158^4 + 59^4 = 133^4 + 134^4 = 635\ 328\ 657$$

is the smallest number that can be written as the sum of two 4th powers written in two different ways.

5.4.2. Congruent Number Problem. One of the oldest questions in number theory uses elliptic curves for its solution. The question can be posed as follows.

Problem. Given an integer n, when is there a right triangle with rational sides that has an area of n? That is, when is $n = ab/2$ for $n \in \mathbb{Z}$ and $a, b \in \mathbb{Q}$, when are a and b the legs of a right triangle?

We will see that the problem of the congruent number n has been turned into a question concerning an elliptic curve. We know that for a right triangle with legs of lengths a and b and hypotenuse with length c,

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

and the area of the triangle is $n = ab/2$. If we let $x = c^2/4$, then

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2}{4} + \frac{ab}{2} = x + n$$
$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \frac{c^2}{4} - \frac{ab}{2} = x - n$$

We see then that x, $x+n$, and $x-n$ are all themselves the square of some rational number, thus their product must still be a square of some rational number y, hence

$$y^2 \quad = \quad x(x+n)(x-n) = x^3 - n^2x$$

Proposition 5.4.1. *Given an elliptic curve E with equation $y^2 = x^3 - n^2x$ and a point P that lies on E, if $2P \neq \infty$, then the x-coordinate of $2P$ is a square.*

Proof. We know that when taking a line tangent to E, and since $2P \neq \infty$, then $2y_1 \neq 0$,

$$m = \frac{3x_1^2 + A}{2y_1} \quad \text{and} \quad x^3 = m^2 - 2x_1.$$

Thus

$$\begin{aligned}
x_3 &= \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1 \\
&= \frac{9x_1^4 + 6Ax_1^2 + A^2}{4y_1^2} - 2x_1 \\
&= \frac{9x_1^4 + 6Ax_1^2 + A^2}{4(x_1^3 + Ax_1)} - \frac{2x_1(4)(x_1^3 + Ax_1)}{4(x_1^3 + Ax_1)} \\
&= \frac{x_1^4 - 2Ax_1^2 + A^2}{4(x_1^3 + Ax_1)} \\
&= \frac{(x_1^2 - A)^2}{4y_1^2}.
\end{aligned}$$

The numerator and denominator are squares, so x_3 is a square.

□

The question of congruent numbers has seen much work, and certain classes of primes have been ruled out, and other classes of primes have been shown to be congruent numbers. Tunnell's Theorem gives partial resolution to the Congruent Number Problem, with one part implying the other. The other direction awaits a proof of the Birch and Swinnerton-Dyer Conjecture, which deals with the open question of whether the rank of an elliptical curve can be arbitrarily large ([20] p.6).

Theorem 5.4.2. *Tunnell's Theorem ([11] p. 221)*

If n is an odd (respectively even), square-free natural number and n is the area of a right triangle with rational sides, then the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$; (respectively for n even, the number of triples of integers (x, y, z) satisfying $4x^2+y^2+8z^2 = \frac{n}{2}$ is equal to twice the number of triples satisfying $4x^2 + y^2 + 32z^2 = \frac{n}{2}$).

If the weak form of Birch-Swinnerton-Dyer conjecture for elliptic curves $E_n : y^2 = x^3 - n^2x$ is true, then these equalities imply that n is a congruent number.

Example 5. Consider if $n = 15$ is a congruent number.

We want to find a triple of rationals $a, b, c \in \mathbb{Q}$ that form a right triangle and have specific area $n = ab/2 = 15$. Therefore we consider the curve where $n = 15$,

$$y^2 = x^3 - 225x. \tag{5.25}$$

It is obvious that $(-15, 0)$, $(0, 0)$, and $(15, 0)$ are all solutions to Eq. (5.25), but the tangents at these points are vertical lines. So when P is any of these three points, then $P + P = \infty$, which is not helpful in finding new points.

A quick search with Excel shows that $x = -9$ produces $y^2 = 1296$, therefore $(-9, 36)$ is a solution. Lines through $(-9, 36)$ and the first three do not produce an x value that is a square, for example $(-15,0)+(-9,36) = (60,-450)$ and $(15,0)+(-9,36) = (\frac{15}{4}, -\frac{225}{8})$; or produced a triplet that was not a set of integers, such as $(0,0)+(-9,36) = (25,100)$ which yielded triple $a = 3\sqrt{10}, b = \sqrt{10}, c = 10$. So, these particular choices of point addition are not helpful.

So we consider the line that is tangent to the curve at $(-9,36)$ to see if we do find an x value that is a square. Using the methods of § 4.3, then slope of the tangent is found by $m = \frac{3x_1^2+A}{2y_1} = \frac{3(-9)^2-225}{2(36)} = \frac{1}{4}$. Then $x_3 = m^2 - 2x_1 = \left(\frac{1}{4}\right)^2 - 2(-9) = \frac{289}{16}$.

Since negative area does not make sense, we want to find $P\star P$ and find the positive y-coordinate. With reflection $y_3 = m(x_1 - x_3) - y_1$, then without reflection $y_3^* = y_1 - m(x_1 - x_3)$. Thus $y_3^* = 36 - \frac{1}{4}\left(-9 - \frac{289}{16}\right) = \frac{2737}{64}$.

Since $x = (c/2)^2$, then $c/2 = 17/4$, and $c = 17/2$.

Recall

$$y^2 = \frac{(a+b)^2}{4}\frac{(a-b)^2}{4}\frac{c^2}{4},$$

thus,

$$y = \frac{(a^2-b^2)c}{8}.$$

Then we find

$$\frac{2737}{64} = \frac{(a^2-b^2)}{8}\cdot\frac{17}{2}.$$

Then $a^2 - b^2 = \frac{161}{4}$. We also know that $a^2 + b^2 = c^2 = \left(\frac{17}{2}\right)^2 = \frac{289}{4}$. When we solve by eliminating b^2, we find $2a^2 = \frac{450}{4}$. Thus, $a = 15/2$ and $b = 4$. We have found a triple of rationals

$$\frac{15}{2}; 4; \frac{17}{2}$$

that form a right triangle and have area 15.

Figure 5.5 shows the line tangent to the curve at the point $(-9,36)$.

5.4.3. Fermat's Last Theorem. An equation of the form $x^2 + y^2 = z^2$ fits the form of the Pythagorean equation $a^2 + b^2 = c^2$. We know that there are infinitely many Pythagorean triples of $a, b, c \in \mathbb{Z}$ that will satisfy the Pythagorean equation. Likewise, the

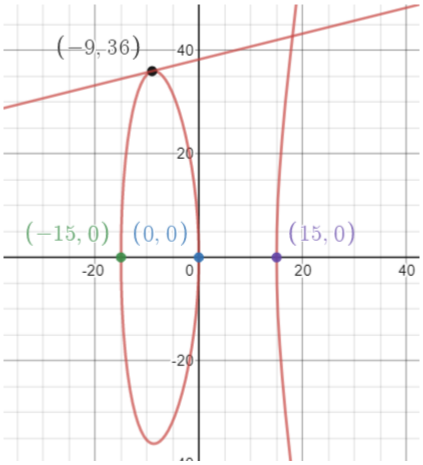


Figure 5.5: $y^2 = x^3 - 225x$

equation $x^2 + y^2 = z^2$ has infinitely many solutions $x, y, z \in \mathbb{Z}$. But it was Fermat who conjectured that for $n > 2$, the equation

$$x^n + y^n = z^n$$

has no triple of nonzero integer solutions. He wrote in the margin of his copy of the works of Diaphantus,

> "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."
>
> Pierre de Fermat, 1637 [5]

Fermat's statement can be summarized below.

Theorem 5.4.3. *Fermat's Last Theorem*

If n is an integer such that $n > 2$, then the equation

$$x^n + y^n = z^n$$

has no solutions when $xyz \neq 0$.

Here, we review a short overview of the developments of the proof of FLT and how that proof is connected to elliptic curves.

From Cox [3], we visit a brief overview of the work done on FLT and its progression. Fermat was able to prove a special case of $n = 4$ using infinite descent. In 1770, Euler attempted to prove the case of $n = 3$, but his proof contained an error which was fixed by Legendre. In 1820's, Sophie Germaine proved a special case of FLT. If $n = p$ and $2p + 1$ are both prime, then $x^p + y^p = z^p$ has no simultaneous non zero integer solutions and $p \nmid xyz$. She also showed in the case of $n = 5$, if the equality $x^5 + y^5 = z^5$ were to hold, then 5 would have to divide one of x, y, or z ([16] p.516). In 1825, Dirichlet and Legendre independently proved the case of $n = 5$ using infinite descent. In 1832, Dirichlet proves the case of $n = 14$. In 1839, Lamé proved the case of $n = 7$ also using infinite descent.

In 1840's Kummer's original work on a problem concerning an area known as quadratic reciprocity turned the question of FLT into a question concerning the nature of cyclotomic numbers (imaginary numbers that satisfy $\zeta^p = 1$ for a prime p). Primes (called regular primes) have the property that the associated ring of cyclotomic numbers has a form of unique factorization. Other primes (called irregular primes) do not allow for that form of unique factorization. Kummer showed that FLT held for regular primes. Unfortunately, although it is known that there are an infinite number of irregular primes, the cardinality of regular primes is not known. This earned him a medal from the French academy in 1856. With help from Vandiver, Kummer showed that FLT held for all $p < 100$. In 1976, Wagstaff showed the FLT held for primes less than 125,000. By 1992, the upper bound for which FLT held had been raised to $p < 4,000,000$ [3].

In 1986, Frey turned the question of FLT into a question about elliptic curves. He studied the equation

$$y^2 = x(x - a^n)(x + b^n) = g(x).$$

Such curves are called *Frey curves.* Although curves of this nature bear Frey's name, he was not the first to discover such curves. The Frey curve was mentioned by French mathematician, Y. Hellegouarche in 1975 regarding FLT and by D. Kubert and Serge Lang in 1985. However, Frey was the first to formalize the idea that the Frey curve could not exist because of the Taniyama-Shimura conjecture which was first partially proposed by Y. Taniyama in 1956 and further refined by G. Shimura in 1957. The Taniyama-Shimura Conjecture has also been called the Taniyama-Shimura-Weil after being reconsidered and expanded by A. Weil in 1967.

It was Frey who conjectured that Frey curves could not possibly be a modular function (a special type of function meeting certain assumptions) because of their special properties. He then made the connection to the Taniyama-Shimura conjecture that, if true, held that all elliptic curves were indeed modular functions. Thus Frey conjectured Frey curves would directly contradict the assumptions of Taniyama-Shimura conjecture (widely held to be true), and a proof thereof would imply that FLT held.

Frey was unable to prove his conjecture. Progress on this conjecture was made by Jean-Pierre Serre and was called the Serre epsilon-conjecture, which made assertions on Galois representations and modularity given certain conditions. In 1990, K. Ribet proved that the Serre epsilon-conjecture was true. A corollary was that Frey curves could not be modular. Also, by extension, he had shown that the Taniyama-Shimura conjecture (TSC) implied FLT for all primes, since if one could prove that elliptic curves could indeed be parameterized by modular forms, then, since Frey curves are elliptic curves, it too could be parameterized by a modular form.

In 1995, Wiles showed that Frey curves were semi-stable (a special property relating the discriminant of a polynomial and its roots). Wiles, with Taylor's help, proved a special case of TSC for semi-stable curves. Since Frey curves can also be shown to be semi-stable, then the special case of TSC says that Frey curves could also be parameterized by modular forms. This indeed showed that Frey curves were a contradiction to TSC which was sufficient to prove FLT [3].

The TSC is now simply called the modularity theorem. After Wiles proved the special case of semi-stable curves in his proof of FLT, Breuil, Conrad, Diamond, and Taylor proved the full modularity theorem in 2001 [24].

6. ELLIPTIC CURVE FACTORING

6.1. Some Methods of Factorization

6.1.1. Brute Force. Given an integer n, this method simply means testing all the primes p such that $p < \sqrt{n}$. This method is the most inefficient and only useful for relatively small numbers.

6.1.2. Fermat Factorization. Again this method is still inefficient, but becomes the basis for other factorization methods. Suppose that there are integers s and t such that $n = s^2 - t^2$. Then $n = (s-t)(s+t)$.

The methodology of Fermat factorization can be described as follows. One, determine $s = \lceil \sqrt{n} \rceil$. Two, compute $s^2 - n = k$. Three, for $k = t^2$, determine if $t \in \mathbb{N}$. Lastly, if $t \in \mathbb{N}$, then the factorization of n is found by $n = (s+t)(s-t)$. Else, take $s + 1 \to s$ and return to step 2.

Example 6. Find a factorization of 6887.

Since $\sqrt{6887} \approx 82.99$, let $s = 83$:

$$83^2 - 6887 = 2$$

$$84^2 - 6887 = 169 = 13^2$$

Thus $s = 84$, $t = 13$, and $6887 = (84 + 13)(84 - 13) = 97 \cdot 71$.

6.1.3. Pollard $p - 1$ Method. This method was developed by John Pollard in 1974 and uses Fermat's Little Theorem as its basis ([16] p. 219).

Theorem 6.1.1 (Fermat's Little Theorem)**.** *If p is prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Since p is prime and $p \nmid a$, then the list of integers $a, 2a, \ldots, (p-1)a$ are not divisible by p. Also, since p is prime, then a has an inverse and no two integers in the list are equal (if $ja \equiv ma \pmod{p}$, then $j \equiv m \pmod{p}$, which is a contradiction to the assumption of the list). Therefore the list of integers $a, 2a, \ldots, a(p-1)$ is equal to some ordering of $1, 2, \ldots, p-1$, and therefore

$$a \cdot 2a \cdots a(p-1) \equiv 1 \cdot 2 \cdots (p-1).$$

There are $p-1$ factors of a on the left, thus after a rearranging:

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

After multiplying both congruence's by the inverse of $(p-1)!$ (which exists since $\gcd((p-1)!, p) = 1$), then $a^{p-1} \equiv 1 \pmod{p}$. □

Let n be a composite number and $n = pq$ for a prime factor p . For some integer a, if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. If $k!$ is the smallest factorial such that $(p-1)|k!$, then $a^{k!} = a^{(p-1)c} \equiv 1 \pmod{p}$ for some integer c. Let $M \equiv a^{k!} - 1 \equiv 0 \pmod{p}$ and let $d = \gcd(M, n)$. In order to be effective, $p-1$ must be the product of small primes, otherwise the iterations described below must be repeated until all the primes of $p-1$ are expressed within $k!$.

We wish to find $k!$ such that $\gcd(a^{k!} - 1, n) \neq 1$. This can be done by taking ever-increasing powers of a modulo p and and performing the Euclidean algorithm with each step to see if we have reached a desired factorization. Let r_k be the step where a is raised the to $k!$ power.

The methodology for the Pollard $p-1$ method can be described as follows. Let n be the number that is to be factored. First, choose a base a. One can choose $a = 2$ initially, but any base will work. Second, perform $r_k = a^{k!} \pmod{n}$, with $k = 2$ initially. Third, compute $\gcd(r_k - 1 \pmod{n}, n) = d$. If $d \neq 1$, then d is a nontrivial factor of n and n can be factored in terms of d. Else, $k + 1 \rightarrow k$ and return to step 2.

Example 7. Find a factorization of 200027.

$$\begin{aligned}
r_2 = 2^{2!} = 2^2 &\equiv 4 \pmod{200027} \quad \text{and} \quad \gcd(3, 200027) = 1 \\
r_3 = 2^{3!} = 4^3 &\equiv 64 \pmod{200027} \quad \text{and} \quad \gcd(63, 200027) = 1 \\
r_4 = 2^{4!} = 64^4 &\equiv 174975 \pmod{200027} \quad \text{and} \quad \gcd(174974, 200027) = 1 \\
r_5 = 2^{5!} = 174975^5 &\equiv 94062 \pmod{200027} \quad \text{and} \quad \gcd(94061, 200027) = 1 \\
r_6 = 2^{6!} = 94062^6 &\equiv 141976 \pmod{200027} \quad \text{and} \quad \gcd(141975, 200027) = 1 \\
r_7 = 2^{7!} = 141976^7 &\equiv 58053 \pmod{200027} \quad \text{and} \quad \gcd(58052, 200027) = 631
\end{aligned}$$

So then 631 is a factor of 200027 and we have a factorization of

$$200027 = 631 \cdot 317.$$

6.1.4. Quadratic Sieve Factorization. A much more powerful tool is the quadratic sieve factorization (QSF) which uses the idea of Fermat factorization. We will give the statement and proof of QSF and then discuss briefly how the process would be used to find a factorization of a number ([7], p. 5).

Theorem 6.1.2 (QSF)**.** *Let $n,\ x,\ y \in \mathbb{N} \setminus 0$. Suppose there exists x, y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. Then $\gcd(x-y, n)$ is a non-trivial factor of n.*

Proof. Let $d = \gcd(x-y, n)$. Then d is a divisor of n and thus $1 \leq d \leq n$. If $d = n$, then n is a divisor of $x - y$ and thus $x - y \equiv 0 \mod n$, which implies that $x \equiv y \mod n$. This contradicts the assumption, thus $d \neq n$.

If $d = 1$, then $n \nmid x - y$. By assumption, $x^2 \equiv y^2 \mod n$, thus $x^2 - y^2 \equiv 0 \pmod{n}$, and $(x+y)(x-y) \equiv 0 \mod n$ and hence $n|(x+y)(x-y)$. Since $\gcd(x-y, n) = 1$, then $n|x+y$. This implies that $x \equiv -y \mod n$, which also contradicts hypothesis, so $d \neq 1$.

Thus $1 < d < n$ and d is a non-trivial factor of n. □

In short, the idea is to find a pair of congruent squares $a, b \pmod{n}$, such that $a \neq \pm b \pmod{n}$, and then use the Euclidean algorithm to find $\gcd(a \pm b, n)$ to find a non-trivial factor. Consider the following congruences:

$$\begin{aligned} x_1^2 &\equiv p_1^{k_{11}} p_2^{k_{12}} \dots p_j^{k_{1j}} \pmod{n} \\ x_2^2 &\equiv p_1^{k_{21}} p_2^{k_{22}} \dots p_j^{k_{2j}} \pmod{n} \\ &\vdots \\ x_i^2 &\equiv p_1^{k_{i1}} p_2^{k_{12}} \dots p_j^{k_{ij}} \pmod{n} \end{aligned}$$

Looking at just the exponents of the right-hand side, the factorizations of congruences of x_i^2 form a matrix (a_{ij}) where each row correspond to the powers of primes of the factorization. If one can find a combination of rows where the sum of each column is even, then product of squares x_i is then equal to a product of squares mod n. Furthermore, if the square-root of the left-hand side is not equal to plus/minus the square root of the right hand side, then we can use the Euclidean algorithm to find the factor.

To keep the square of numbers that need to be factored small, it is common to use $\lfloor\sqrt{mn}+r\rfloor$ as candidates for x_i. Here, m and r are arbitrary integers, but it seems fruitful to use increasing primes for m and to use $r = 1$, until one can find a sum of rows that has the desired results.

Here, we describe the methodology in using QSF. Let n be the number to be factored. Choose integers m and r. Initially, one can choose $r = 1$ and $m = 2$. For each m, (one can choose successive primes), compute $s_m = \lfloor\sqrt{mn}+r\rfloor$ and then find the prime factorization $s_m^2 = p_1^{k_{i1}} p_2^{k_{i2}} \cdots p_i^{k_{ij}} \pmod{n}$. Choose rows of s_m^2 so that $\sum k_{ij} \in 2\mathbb{Z}$ for each j. Therefore $\Pi s_m^2 = y^2$. Then compute $D = \prod s_m - y \pmod{n}$ for the chosen m. Lastly, compute $\gcd(D, n)$. This is a nontrivial factor of n.

Example 8. Find the factorization of 410027.

Table 6.1 shows some choices for m, s_m, $s_m^2 \pmod{n}$, and the factorization f of s_m^2. Notice then that for lines $m = 59,\ 71,\ 89,$

Table 6.1: Quadratic Sieve Congruences

m	s_m	$s_m^2 \pmod{n}$	f
59	4919	4968	$2^3 \cdot 3^3 \cdot 23$
61	5002	8357	$61 \cdot 137$
67	5242	6755	$5 \cdot 7 \cdot 193$
71	5396	4899	$3 \cdot 23 \cdot 71$
73	5472	10813	$11 \cdot 983$
79	5692	6731	$53 \cdot 127$
83	5834	3315	$3 \cdot 5 \cdot 13 \cdot 17$
89	6041	1278	$2 \cdot 3^2 \cdot 71$

$$\begin{aligned}
4919^2 \cdot 5396^2 \cdot 6041^2 &\equiv (2^3 \cdot 3^3 \cdot 23)(3 \cdot 23 \cdot 71)(2 \cdot 3^2 \cdot 71) \pmod{410027}\\
(4919 \cdot 5396 \cdot 6041)^2 &\equiv 2^4 \cdot 3^6 \cdot 23^2 \cdot 71^2 \pmod{410027}\\
4919 \cdot 5396 \cdot 6041 &\equiv 2^2 \cdot 3^3 \cdot 23 \cdot 71 \pmod{410027}\\
235237 &\equiv 176364 \pmod{410027}.
\end{aligned}$$

Subtracting $235237 - 176364 = 58873$. Lastly, $\gcd(58873, 410027) = 521$ and by the theorem, 521 is a nontrivial factor of 410027. We find the factorization

$$521 \cdot 787 = 410027.$$

6.1.5. Number Field Sieve. The best algorithm for factoring large numbers (numbers over 115 decimal digits) is the number field sieve. However, the factorization of 1024-bit numbers which are now common with RSA systems would still take thousands of years of computing time to factor any one random 1024-bit (309 decimal-digit) number. The theory of this method is beyond the scope of this thesis ([16] pp. 125-6).

6.1.6. Shor's Algorithm. The most efficient algorithm would be Shor's algorithm, but this requires the use of quantum computers. If quantum computers ever become a challenge to today's bit-computers, then quantum computers can factor large numbers in polynomial time and would be a threat to our current encryption methods. Quantum computers could defeat the discrete logarithm problem (see § 7.3.1) and integer factorization problem, but such feats seem to be a long way off, if ever. The largest number factored by a quantum computer so far is $1,099,551,473,989 = 1,048,589 \cdot 1,048,601$ in December 2019 [4].

6.2. Elliptic Curve Factorization

6.2.1. Usefulness. Elliptic curve factorization (ECF) is a fast, intermediate method when factoring integers of 50 to 60 digits and most commonly used to pull out small divisors (up to 20 to 30 digits) of a large integer ([22], [20] p. 180). Pollard's $p-1$ method may be useful for factoring numbers up to 10^7, the quadratic sieve up to 10^{75}, and number sieve for numbers beyond that. These bounds are not hard and fast as to what researchers and computer programmers employ when deciding which algorithms to use when factoring numbers, this fact is simply mentioned to give an idea of when different algorithms are put into effect. ECF is also useful that it can be run in parallel. As we will see below, several curves to be explored can be built and tested at the same time. This allows the algorithm to be run on several processors at once and to gain results in a reasonable amount of time.

6.2.2. ECF Overview. For a curve E in Weierstrass form, when computing slope $dy/dx = u/v \pmod{n}$ for some n, one must compute $v^{-1} \pmod{n}$. If no such inverse exists, then v is not invertible, so $\gcd(v, n) \neq 1$ and v and n share a common factor. For an n that one wishes to factor, the goal of ECF is took look for non-invertible elements $v \pmod{n}$ and then compute $\gcd(v, n)$ to find a non-trivial factor of n.

For example, consider the following elliptic curve E

$$y^2 = x^3 + 3x \pmod{15}$$

Consider the case of $P = (9, 9)$. In order to find $2P$, we must first find the slope m. We know that

$$2y\ dy = (3x^2 + 3)dx \pmod{15} \Rightarrow 3\ dy = 6dx \pmod{15}.$$

In order to find the slope, we must first multiply by the inverse of 3, however $\gcd(3, 15) \neq 1$. Thus there is no inverse, and 3 is non-invertible. We calculate $\gcd(3, 15) = 3$ and 3 is a non-trivial factor of 15. We find then that 15 is factored as $15 = 3 \cdot 5$. This method requires one to use enough elliptic curves E_i mod the desired n and enough starting points P_i on the curves to find a point where one finds non-invertibility.

Here, we describe the steps to perform ECF.

Elliptic curves can be easily constructed by choosing parameters, A, u, and v and computing

$$B = v^2 - u^3 - Au. \pmod{n} \tag{6.1}$$

Thus, if we let $u = x$, and $v = y$, then we have created elliptic curve $E = y^2 = x^3 + Ax + B \pmod{n}$ in normal Weierstrass form modulo a chosen integer. The algorithm calls for several curves to be constructed and tested simultaneously. We can let each E_i correspond to parameters (u_i, v_i, A_i). For example, working with modulus 29, the reader can verify that the parameters $(u_1, v_1, A_1) = (10, 1, 3)$ produce the curve $E_1 = y_1^2 = x^3 + 3x + 15 \pmod{29}$ with rational point $(10, 1)$.

Recall that for an elliptic curve E written in normal Weierstrass form, for a given point P, one can easily find $2P$ using the formulas previously outlined. By using this doubling algorithm, one can compute any 2-power multiple of P. Thus if we can easily determine $2P$, then we can just as easily determine $4P$, $8P$, $16P$, etc. Recall, also, that there is a binary expression for any integer. Thus with the doubling of points, any k-multiple of P can be found by adding the appropriate powers of 2 multiples of P that sum to kP. In this manner, $C!P$ can be also be found. As an example, if one wanted to find $23P$, then

$23P = 16P + 4P + 2P + P$.

Let E be an elliptic curve defined by equation written $y^2 = x^3 + Ax + B \pmod{n}$ with primes p and q dividing n. Let P be a point that lies on E. Then, we also have

$$y^2 = x^3 + Ax + B \pmod{p} \quad \text{and} \quad y^2 = x^3 + Ax + B \pmod{q}.$$

Recall also that by Hasse's theorem, $N_p = \#E(\mathbb{F}_p)$ falls between $p+1-2\sqrt{p} \leq N_p \leq p+1+2\sqrt{p}$, with N_p happening with uniform randomness. Likewise, this holds for $N_q = \#E(\mathbb{F}_q)$. Because of N_p and N_q happening equally randomly within their respective Hasse intervals, the chances of N_p and N_q containing larger primes that divide both is low.

Let P have order k in $E(\mathbb{F}_p)$. Then $kP = \infty$ and $k|N_p$. Moreover, $N_pP = \infty$ and $(tN_p)P = \infty$ for any t-multiple of N_p. Likewise, say P has order m in $E(\mathbb{F}_q)$. Then $mP = \infty$, and $m|N_q$. Also, $N_qP = \infty$, and $(sN_q)P = \infty$ for any s-multiple of N_q. Because of the likelihood that N_p and N_q contain different primes, then without loss of generality, there is likely a small $C!$ such that $k|C!$, but $m \nmid C!$. Then $C!P = \infty \pmod{p}$, but $C!P \neq \infty \pmod{q}$, a contradiction that will express itself as for $dy/dx = u/v$, then $\gcd(v, p) \neq 1$ (v is non-invertible is $\mathbb{F}_p$) while $\gcd(v, q) = 1$ (q remains invertible in $\mathbb{F}_q$) . Then $\gcd(C!, n)$ is a non-trivial factor of n.

If none of the $C!P$ induce elements for any E_i, then one can continue to increase C or choose new E_i and repeat the process.

6.2.3. Example. Find a factorization of 332977.

For parameters $(u_1, v_1, A_1,)$, we chose $(10, 1, 3)$. After substituting into (6.1), this yields $B = 331948$. Thus

$$E_1 = (10, 1, 3) \Rightarrow y^2 = x^3 + 3x + 331948.$$

Before finding $C!$, we find doubled points of $P = (10, 1)$ such as $2P = (272665, 148403)$, $4P = (16212, 288709)$, etc. up to whatever 2^k-multiple of P is necessary till a contradiction is reached.

Calculating up to $9!P$, we find the following

$$\begin{aligned}
2!P = 2P &= (272665, 148403) \\
3!P = 6P &= 2P + 4P \\
&= (216731, 197614) \\
4!P = 24P &= 16P + 8P = \\
&= (257684, 150650) \\
5!P = 120P &= (64P + 32P) + 16P + 8P \\
&= (255384, 188904) \\
6!P = 720P &= (512P + 128P) + 64P + 16P \\
&= (244293, 261270) \\
7!P = 5040P &= (4096P + 512P) + 256P + 128P + 32P + 16P \\
&= (71093, 179000) \\
8!P = 40320P &= 32768P + 4096P + 2048P + 1024P + 256P + 128P \\
&= (320501, 59583) \\
9!P = 362880P &= [262144P + 65536P] + 32768P + 2048P + 256P + 128P \\
&= (294766, 283642) + (193877, 155420)
\end{aligned}$$

When trying to find the slope between these two points in order to find point addition, we find that $x_1 - x_2 = 294766 - 193877 \equiv 100899 \pmod{332977}$. After performing the Euclidean algorithm in order to find $100899^{-1} \pmod{332977}$, we find $\gcd(100889, 332977) = 433$. Thus we have found a factor of 433 and we find

$$332977 = 433 \cdot 769.$$

If this choice of elliptic curve had not worked, we could have used other curves until we succeeded.

6.3. Primality Testing

6.3.1. Remarks. No algorithm that can factor an integer in polynomial time is known to exist, and it has not yet been proven (and it is widely believed) that no such algorithm does exist. The largest integer factored that is not of a special form is RSA-250, a 250 decimal digit integer that was factored in February 2020 and took 2700 core-hours [26]. In fact the largest of the RSA numbers, RSA-2048, a 2048 bit, 617 decimal-digit number, may not be factorable for the next century with current bit-computing. A quantum computer (if even possible) could factor RSA-2048 in less than 24 hours, but that capability may still be ten to twenty years from this writing.

There are algorithms that can test a number's primality in polynomial time. They can test integers that are much larger than those that have been factored [25]. Some tests can test numbers with several hundred digits, but elliptic curve primality testing is the most popular and can test random integers not of a special form with over a thousand decimal-digits ([20] p. 184).

If a primality test states that a number is composite, it does not necessarily produce a factorization; it only says that an integer is composite. If p is the number that is being tested for primality, and for some base $a^{p-1} \not\equiv 1 \pmod{p}$, then we conclude p is composite. Integers that continually pass pseudo-primality tests (that is, fail to show that they are composite) are probably prime. The more tests that they pass, the more the probability increases that they are prime.

6.3.2. Pocklington-Lehmer Primality Testing. The Pocklington-Lehmer test is restated and proved below with the help of Washington ([20] pp. 184-5).

Theorem 6.3.1 (Pocklington-Lehmer)**.** *Let $n > 1$ be an integer, and let $n - 1 = rs$ with $r \geq \sqrt{n}$. Suppose that, for each prime $l|r$, there exists an integer a_l with*

$$a_l^{n-1} \equiv 1 \pmod{n}, \quad \textit{and} \quad \gcd\left(a_l^{(n-1)/l} - 1, n\right) = 1.$$

Then n is prime.

Proof. Let p be a prime factor of n, then $n = pk$, for some k. Let l^e be the highest power of each prime l that divides r. Let $b_l \equiv a_l^{(n-1)/l^e} \pmod{p}$. Then $b_l^{l^e} \equiv a_l^{n-1} \equiv 1 \pmod{p}$. Since $a_l^{(n-1)/l} \not\equiv 1 \pmod{pk}$, therefore $b_l^{l^{e-1}} \not\equiv 1 \pmod{pk}$. Then $\operatorname{ord}(b_l) \pmod{p} = l^e$. Since $b_l^{p-1} \equiv 1 \pmod{p}$, then $l^e | p-1$ by Lagrange's Theorem. Since this is true for every $l^e | r$, then $r | p-1$. Therefore, $p > r$, and thus $p > r \geq \sqrt{n}$. Since p is a prime factor and n is larger than n that would be at most $\sqrt{n}$, then $p = n$ and n is prime. □

6.3.3. General Form Example. Prove that 140681 is prime.

First, subtract 1, then $140681 - 1 = 140680 = 2^3 \cdot 5 \cdot 3517$. To use the theorem above, we let $r_1 = 3517 > \sqrt{140681} \approx 375.1$. If we were not sure that r_1 is prime or that we have a complete prime factorization, then we can use the theorem again on factors that need their primality verified. Suppose that we need to verify that r_1 is indeed prime, then we can reiterate the theorem again. Thus, $3517 - 1 = 3516 = 2^2 \cdot 3 \cdot 293$. We let $r_2 = 293 > \sqrt{3517} \approx 59.3$. Let's say we were not sure if 293 was prime, so we iterate the theorem one more time so that $293 - 1 = 292 = 2^2 \cdot 73$. We will let $r_3 = 73 > \sqrt{293} \approx 17.1$. Suppose that we are now confident that we have a factor r_3 that is prime (or any other cases have a complete prime factorization). Now we can use the theorem to build back up to the original question. We use the fact that 73 is prime (we have all the prime factors of r_2) to show that 293 is prime, thus we have all the prime factors of r_1 to show that 3517 is prime, which we then can use to show that n is prime.

So first, we prove 293 is prime by making sure we have met the assumptions of the hypothesis. Since $r = 73$, we need only test 73. For large calculations, we can create algorithms that use succesive doublings and a binary representation of the number we wish to test.

$$2^{292} = 2^{256} \cdot 2^{32} \cdot 2^{4} \cdot \equiv 1 \pmod{293}, \quad \text{and} \quad \gcd(2^{292/73}, 293) = 1$$

Since $r_3 = 73$, and 73 is prime, then conditions of hypothesis are met and 293 is prime.

Now we use the conditions of the hypothesis to test if 3517 is prime.

$$2^{3516} \equiv 1 \pmod{3517} \quad \text{and} \quad \gcd(2^{3516/293}, 3517) = 1.$$

Since $r_2 = 293$ and 293 is prime, then $l = 293$ is the only l needing to be tested. Again the conditions of the hypothesis are met and 3517 is prime.

Lastly, $r_1 = 3517$ and 3517 is prime, so $l = 3517$, is the only one to be tested:

$$2^{140680} \equiv 1 \pmod{140681} \quad \text{and} \quad \gcd(2^{140680/3517}, 140681) = 1.$$

Thus the hypothesis are satisfied and 140681 is prime.

6.3.4. Remarks on Pocklington-Lehmer Method. Notice that the hypothesis was used several times to prove that we had all the prime factors of r. While testing the primality of extremely large numbers, it may be necessary to show the primality of resulting $l|r$.

The hypothesis of the theorem supposes that one can find factorization of $n - 1$ (it need not be complete) so that one assumes that enough small factors of $n - 1$ can be divided out such that one can derive an r such that $r > \sqrt{n}$. When dealing with extremely large n of say a thousand decimal digits (and since factoring is a non-trvial process), then $n - 1$ may not have a readily apparent factorization. It might be that $n - 1$ is the product of two 500 decimal-digit integers, or three 300+ decimal digit integers, or four 250-decimal integers, and so on, cases where factorization is not easily obtained. To this extent, then elliptic curves come to play. They are the next method to use when the above method does not work.

6.3.5. Elliptic Curve Theorem. This theorem uses the fact that $\#E(\mathbb{F}_p)$ is close to the order of $\mathbb{Z}_p^\times$ which has order $p - 1$, the number that we are trying to factor. If we are able to find enough primes p_i, such that for a finite point $P \in E(\mathbb{Z}_n)$ such that $p_1 P = \infty$, then we can gather enough information to show that n is prime. The algorithm shown below is taken from Washington ([20] p. 186).

Theorem 6.3.2 (Goldwasser-Kilian Primality Algorithm)**.** *Let $n > 1$ and E be an elliptic curve mod n. Suppose there exist distinct prime numbers $l_1, \ldots, l_k$ and finite points $Pi \in E(\mathbb{Z}_n)$ such that*

1. $l_i P_i = \infty\ for\ 1 \leq i \leq k,$
2. $\prod_{i=1}^{k} l_i > (n^{1/4} + 1)^2.$

Then n is prime.

Proof. Let p be a factor of n. Then write $n = p^f n_1$ for some exponent f of p such that $p \nmid n_1$. Then

$$E(\mathbb{Z}_n) = E(\mathbb{Z}_{p^f}) \oplus E(Z_{n_1}).$$

Let P_i be a finite point of $E(\mathbb{Z}_n)$. Then P_i is a finite point of $E(\mathbb{Z}_{p^f})$ and furthermore, also a finite point of $E(\mathbb{F}_p)$. Then since P_i has finite order in $E(\mathbb{Z}_n)$, then $l_i P_i = \infty \pmod{n}$ for some prime l_i, then $l_i P_i = \infty$ for any factor of n. So $l_i P_i = \infty \pmod{p}$. Thus l_i divides order of the group $E(\mathbb{F}_p)$, that is $l_i | \# E(\mathbb{Z}_p)$ for all i, thus $\prod l_i | \# E(\mathbb{F}_p)$. Thus the following inequality shows:

$$(n^{1/4} + 1)^2 < \prod_{i=1}^{k} l_i \leq \# E(\mathbb{F}_p) < p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2.$$

Thus $p > \sqrt{n}$. Since n has a non-trivial factor at most $\sqrt{n}$, and p is prime, then n is prime. □

6.3.6. Elliptic Curve Example. Determine if 331 is a prime number.

First we must choose an elliptic curve mod 331 and determine its group order. Let's choose

$$y^2 = x^3 + 2x - 11 \pmod{331}.$$

Earlier, when reviewing BSGS, we found that the order of this group was 335. Consider the point $P = (268, 48)$. We find that $67P = \infty$. We also find that this is the only prime l which induces the identity for this point. Now we consider $(q^{1/4} + 1)^2 \approx 27.7$. Since $\prod l_1 = 67 > (q^{1/4} + 1)^2 \approx 27.7$, then we conclude that 331 is prime.

7. ELLIPTIC CURVE CRYPTOGRAPHY

7.1. Introduction and Definitions

Cryptography is the science of sending and receiving messages with confidence that the chances of the messages being intercepted are extremely low. Here, we discuss some basic terminology related to cryptography. Then we discuss the key that keeps cryptography safe, that is, the discrete logarithm and its counter-part as it relates to elliptic curves; some methods of encryption, especially those that relate to elliptic curves; and some methods (attacks) that are used to attempt to decode messages.

The legitimate players are involved in the act of sending and decoding messages (the ones that are sending the messages and the ones who are the intended receivers) are normally called Alice and Bob. If an algorithm that involves a third legitimate party, he is called Chris. Any information sent by Alice is denoted with an A, or a subscript a depending on notation; information from Bob is denoted with B, or b; and information from Chris is denoted with C or c.

The illegitimate player, the one who is trying to intercept messages not intended for her, she is called Eve (short for eavesdropping). We can always assume that Eve has the knowledge and computing capability to intercept any sent message. Thus any created cryptographic algorithm must be strong enough to resist Eve's attacks.

The text that is meant to be read by messenger is called *plaintext.* This is usually denoted with a P. This is the message that is needs to be protected. Messages that encrypted are called the *ciphertext.* These are usually denoted with a C. These are the messages that need algorithms strong enough that Eve cannot decipher them.

7.2. Types of Cryptographic Systems

7.2.1. Private Key Systems. Private key systems are ones where Alice and Bob have a key in advance of the message. They have communicated before the message was sent and developed a key that can be used to encode and decode the text. A simple such system would be a mono-alphabetic system. If Alice encodes each letter of the alphabet to the next one (A is sent to B, B to C, C to D, etc.), then Bob know that when he receives the message, he sends each letter backwards to the previous letter). The security of the message depends on Eve not being able to deduce the key in a reasonable amount of time.

There are other types of private key systems. An interesting example is the Enigma machine used by the Germans in WWII, and was featured in a movie *The Imitation Game* (2014) starring Benedict Cumberbatch as the mathematician Alan Turing. The Enigma used rotors that scrambled the letters of the alphabet such as in an alphabet cipher described above, but the circuitry of the machine would send keep sending letters to other characters so that any one letter was not repeatedly sent to itself. The period of when patterns would start repeating was 16900 characters which was much longer than any one sent message. Finding the length of such a period is key when deciphering such system. With the right settings, Enigma messages were equivalent to 67-bit messages. Since the rotor settings were reset everyday at midnight, the security of the system depended on Eve not being able to determine the correct rotor settings within any given 24-hour period. It has been said that had the Germans used “good” practices, then Enigma would have been “unbreakable.” Inherent weaknesses in the methodology and the practices of the Germans allowed the Allied powers to intercept and read German messages thus helping to end the war [21].

Other systems such as Data Encryption Systems (DES) and Advanced Encryption systems (AES) are private-key systems. These types of systems are called **symmetric encryption**. These systems are much quicker than **public key encryption**.

7.2.2. Public Key Systems. These systems are called **asymmetric encryption**. These systems allow for the exchange of information without having to have met beforehand. Alice can send a message to Bob, with her signature on it, and Bob can verify that it was indeed that Alice was the one that sent the message and can decrypt the message.

These messages depend on the fact that the decryption process cannot be found in a reasonable amount of time. In this way, the algorithm for encrypting and the encrypted message can be "broadcasted" because the assumption is that even with Eve's most powerful tools, she will not be able to decipher the original message. These public algorithms are more computationally involved, thus take longer and require more storage to transmit.

Because asymmetric systems are slower than symmetric ones, sometimes one will opt to send a symmetric key via an asymmetric transmission. Then only the new private-key need be decoded using the slower public-key, and then information between two parties can then be exchanged with their private-key system. In this way, the slower public-key encryption allows two parties to exchange information for their private-key encryption without having to worry about the security of their private key in the exchange.

7.2.3. RSA Encryption. One of the most well-known public key systems is the one developed by Rivest, Shamir, and Adelman in 1977. This algorithm uses modular arithmetic and Fermat's Little Theorem. RSA uses the apparent difficulty of the integer factorization problem for its security. Sufficiently large numbers apparently cannot factored in a reasonable time. As mentioned before, it maybe take centuries for a random 2048-bit number can be factored. Note that viable quantum computers would make factoring easy and would therefore defeat RSA.

To send messages using RSA, large primes p and q are chosen and then $n = pq$ is determined. From these primes, the number $k = (p-1)(q-1)$ is determined, and then some number d is chosen so that $\gcd(d, k) = 1$ and then $e = d^{-1} \pmod{k}$ is determined. Then numbers n and e are announced, but p, q, d are kept secret. A message M can be encoded by $M^e \pmod{n}$. The message is decoded by $(M^e)^d = M \pmod{n}$. The message remains secure by the apparent difficulty of factoring n so that k cannot be easily determined and therefore d cannot be easily determined.

RSA works by the following theorem [10].

Theorem 7.2.1. *Let $n = pq$ and $k = (p-1)(q-1)$ for primes p, q. For integer d, let $\gcd(d, k) = 1$ and let $e = d^{-1} \pmod{k}$. Then for every $b \in Z$,*

$$b^{ed} \equiv b \pmod{n}.$$

Proof. Since e is a solution of $dx \equiv 1 \pmod{k}$, then $ed - 1 \equiv 0 \pmod{k}$ and $ed - 1 = kt$ for t-multiples of k. Then,

$$b^{ed} = b^{kt+1} = b^{(p-1)(q-1)t}b.$$

If $p \nmid b$, then $b^{(p-1)(q-1)t}b = 1^{(q-1)t}b = b \pmod{p}$ by Fermat's Little Theorem. If $p|b$, then $b \equiv 0 \pmod{p}$ and $b^{ed} = b \pmod{p}$ in all cases. Similarly, $b^{ed} \equiv b \pmod{q}$ in all cases.

Lastly, since $p|b^{ed} - b$ and $q|b^{ed} - b$, then $pq|b^{ed} - b$. Thus n divides $b^{ed} - b$ Therefore $b^{ed} \equiv b \pmod{n}$. □

Sometimes a receiver of a message wants to verify that the message is from the proper sender (not an imposter posing as the sender). This verification of the sender is called a digital signature, a separate message from the encrypted message that the sender uses to verify the authenticity of the encrypted message. For RSA, a hashing function $hash$ is used on m to generate $hash(m) = h$. Then the sender performs $h^d = s$ and sends signature s along with m to the receiver. The receiver then takes m and uses the same hashing function and performs $hash(m)$. The receiver then performs $s^e = h_2$. The receiver then analyzes h_2 and h and if $h_2 = h$, then they conclude that m is an authentic message from the intended sender [13]. This is true since

$$h^{de} = (h^d)^e = s^e = h \pmod{n}.$$

7.3. Logarithm Problems

The likewise apparent difficulty of the discrete logarithm problem is what makes these systems secure.

7.3.1. Discrete Logarithm Problem (DLP). Given a, b, and p, solve the following equation

$$a^k \equiv b \pmod{p}$$

for k (assuming that a solution exists) ([20] p. 133).

7.3.2. Elliptic Curve Discrete Logarithm Problem (ECDLP). Given an elliptic curve E defined over a field for some prime, $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order n, and a point $Q \in \langle P \rangle$, find an integer $\ell \in [0, n-1]$ (if it exists) such that $Q = \ell P$ ([8] p. 153).

7.3.3. Elliptic Curve Diffie-Helman Problem (ECDHP). Given P, aP, bP in $E(\mathbb{F}_q)$, find abP ([20] p. 161).

Here, we note that this is not $aP + bP$. This requires the use of discrete logs. If Eve can solve discrete logs over $E(\mathbb{F}_q)$, then given P and aP, she can find a (or she can use P and bP to find b). She can then multiply bP by a to obtain abP (or she can multiply aP by b to obtain the same).

7.3.4. Decision Diffie-Helman Problem (ECDDHP). Given P, aP, and bP in $E(\mathbb{F}_q)$ and a given point $Q \in E(\mathbb{F}_q)$, decide if $Q = abP$.

7.3.5. A Note on Logarithm problems. It is not known if ECDLP can be reduced to a polynomial time algorithm. Interestingly, the proof of a non-existence of a polynomial-time algorithm for ECDLP would prove that $P \neq NP$, one of the still outstanding, unsolved Millenial Problems ([8], p. 154).

7.4. Attacks on DLP and ECDLP

7.4.1. Index Calculus. This section describes the attack on DLP explained in Washington ([20] pp. 134-5).

Given $g,\ h \in \mathbb{Z}_p$, find k such that $g^k = h$.

Let $g \in \mathbb{Z}_p$ be a primitive root. That is, for $g \in \mathbb{Z}_p^\times$ (a multiplicative group), then $\text{ord}(g) = p-1$. In other words, for every $h \in \mathbb{Z}_p$ and $h \not\equiv 0 \pmod{p}$, then $h = g^k \pmod{p}$ for some non-zero integer k. We define the **discrete logarithm** of h with respect to g as $L(h) = k$.

Since g is a primitive root based on its order within the multiplicative group $\mathbb{Z}_p^\times$ (that is $g^{p-1} \equiv 1 \pmod{p}$), L is determined by its value modulo $(p-1)$. Suppose that $g^{k_1} = h_1$ and $g^{k_2} = h_2$. Then $L(h_1) = k_1$ and $L(h_2) = k_2$ and

$$g^{L(h_1h_2)} \equiv h_1h_2 \equiv g^{k_1}g^{k_2} \equiv g^{k_1+k_2} \equiv g^{L(h_1)+L(h_2)} \pmod{p}.$$

Hence,

$$L(h_1h_2) = L(h_1) + L(h_2) \pmod{p-1}.$$

Also, note that $g^{(p-1)/2} \equiv -1 \pmod{p}$. Therefore $(p-1)/2 \equiv L(-1) \pmod{p-1}$.

We use the following procedure to determine k.

In trying solve for k in the congruence $g^k \equiv h \pmod{p}$, we want to take g raised to some different powers such that the representatives of g^{k_i} is the product of a fixed set B of primes. Using the L function turns these products into sums. Using enough powers of g, we determine $L(p_j)$. Given,

$$\begin{aligned}
g^{k_1} &\equiv p_1^{e_{11}}p_2^{e_{12}}\dots p_j^{e_{1j}} \pmod{p}\\
g^{k_2} &\equiv p_1^{e_{21}}p_2^{e_{22}}\dots p_j^{e_{2j}} \pmod{p}\\
&\vdots\\
g^{k_1} &\equiv p_1^{e_{i1}}p_2^{e_{i2}}\dots p_j^{e_{ij}} \pmod{p},
\end{aligned}$$

we then apply the L function to both sides of equivalences and find that

$$\begin{aligned}
k_1 &\equiv e_{11}L(p_1) + e_{12}L(p_2) + \cdots + e_{1j}L(p_j) \pmod{p-1} \\
k_2 &\equiv e_{21}L(p_1) + e_{22}L(p_2) + \cdots + e_{2j}L(p_j) \pmod{p-1} \\
&\vdots \\
k_i &\equiv e_{i1}L(p_1) + e_{i2}L(p_2) + \cdots + e_{ij}L(p_j) \pmod{p-1}.
\end{aligned}$$

If possible, we solve this system for each $L(p_i)$. Here, it is worth mentioning since the system of equations is constrained by the size of choice of B. If B is too small, then there may not be enough information to solve the system of equations. If B is too big, the system can become extremely large and such matrix calculations become cumbersome for some systems.

Next, we take take $h \cdot g^l \pmod{p}$ for several random l until we find a product of primes for whom we have determined a value for each $L(p_i)$ so that

$$h \cdot g^l \equiv p_1^{e_1} p_2^{e_2} \ldots p_j^{e_j} \pmod{p}.$$

Lastly, we then applying the L function to find k.

$$k = L(h) \equiv e_1 L(p_1) + e_2 L(p_2) + \cdots + e_j L(p_j) - l \pmod{p-1}.$$

Example 9. Given, $12^k \equiv 1000 \pmod{1627}$, find k.

First $p - 1 = 1626$. We can assume that we know the factorization of 1626, which is $2 \cdot 3 \cdot 271$. Also g is primitive root of G if $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all $q|p-1$. Then

$$12^{1626/271} = 12^6 \equiv 439 \pmod{1627}$$

$$12^{1626/3} = 12^{542} \equiv 1362 \pmod{1627}$$

$$12^{1626/2} = 12^{813} \equiv 1626 \pmod{1627}$$

Thus, 12 is a primitive root. After searching some small exponents, we find the following.

$$\begin{aligned} 12^{54} &\equiv 11 \pmod{1627} \\ 12^{69} &\equiv -169 \pmod{1627} \\ 12^{10} &\equiv 39 \pmod{1627} \end{aligned}$$

This gives way to the following.

$$\begin{aligned} 54 &\equiv L(11) \pmod{1626} \\ 69 &\equiv L(-1) + 2L(13) \pmod{1626} \\ 10 &\equiv L(3) + L(13) \pmod{1626} \end{aligned}$$

Solving for the second equation, since $L(-1) \equiv 813 \pmod{1626}$ in this case, then $69 - 813 = -774 \equiv 882 \equiv 2L(13) \pmod{1626}$, thus $L(13) = 441 \pmod{1626}$. The third equation becomes $10 \equiv L(3) + 441 \pmod{1626}$, so $-431 \equiv 1195 \equiv L(3) \pmod{1626}$. Next we take $1000 \cdot 12^l$ for various values of l and the reader can verify that

$$1000 \cdot 12^{13} = 33 \pmod{1627}$$

Thus

$$L(1000) + 13 \equiv L(3) + L(11) \pmod{1626}.$$

Then $L(1000) = 1195 + 54 - 13 = 1236 \pmod{1626}$ and indeed

$$12^{1236} \equiv 1000 \pmod{1627}.$$

7.4.2. Baby-Step, Giant Step. Given points $P,\ Q$ on elliptic curve E such that $\#E(\mathbb{F}_q) = N$, find k such that $Q = kP$.

Here, the algorithm for determining k is similarly to the algorithm explained previously in § 5.3.1 for finding the order of a point. First, choose m such that $m > \sqrt{N}$. Then calculate $Q - jmP$ for $j = 0, 1, \ldots, m-1$. These points cycle through the group in big jumps (Giant Step); meanwhile, compute iP for $i = 0, 1, 2, \ldots, m$. These constitute small jumps (Baby Step), we compare the lists until we have a match in x-coordinate. If the y-coordinates are equal, then we conclude that $Q - jmP = iP$. If the y-coordinates are opposites, then conclude that $Q - jmP = -iP$ and then conclude $k = \pm i + jm \pmod N$.

Notice that the algorithm requires that two separate lists be stored. We will see that Pollard's ρ method takes about as many steps as BSGS. However BSGS requires lots of storage, which is one of its disadvantages. Notice that it is not necessary to calculate the order of N. This saves steps and time. BSGS is useful for calculating moderately-sized N, but storage space needed grows as N grows.

Example 10. Suppose the elliptic curve E is given by

$$y^2 = x^3 + 3x + 318 \pmod{331}$$

and $P,\ Q \in E(\mathbb{Q})$ such that $P = (2, 1)$ and $Q = (188, 27)$ and $Q = kP$. Find k.

First, $\sqrt{331 + 1 + 2\sqrt{q}} \approx 19.2$, so choose $m = 20$.

Second, we list of multiples of iP as seen in Table 7.1, for $i = 0, 1, 2, \ldots, m - 1$.

Table 7.1: Baby Steps of BSGS Attack

iP	iP	iP	iP
$0P = \infty$	$P = (2, 1)$	$2P = (135, 160)$	$3P = (247, 281)$
$4P = (9, 322)$	$5P = (268, 48)$	$6P = (317, 74)$	$7P = (91, 12)$
$8P = (132, 35)$	$9P = (223, 206)$	$10P = (329, 142)$	$11P = (22, 42)$
$12P = (269, 64)$	$13P = (84, 28)$	$14P = (217, 126)$	$15P = (192, 4)$
$16P = (232, 187)$	$17P = (50, 130)$	$18P = (272, 225)$	$19P = (287, 20)$

Next we see in Table 7.2 the difference $Q - jmP$ for $j = 0, 1, 2, \ldots m - 1$. Note that for $nP_i = (x_i, y_i)$, then $-nP_i = (x_i, -y_i)$. So $Q - nP = Q + (-nP)$. These calculations are verifiable on an online elliptic curve calculator [1].

Table 7.2: Giant Steps of BSGS Attack

jmP	Q-jmP	jmP	Q-jmP
$0P = \infty$	$Q - 0P = (188, 27)$	$20P = (195, 273)$	$Q - 20P = (150, 94)$
$40P = (294, 292)$	$Q - 40P = (172, 56)$	$60P = (65, 210)$	$Q - 60P = (178, 73)$
$80P = (36, 270)$	$Q - 80P = (260, 233)$	$100P = (63, 48)$	$Q - 100P = (226, 215)$
$120P = (126, 138)$	$Q - 120P = (81, 167)$	$140P = (276, 101)$	$Q - 140P = (222, 203)$
$160P = (144, 11)$	$Q - 160P = (129, 39)$	$180P = (271, 44)$	$Q - 180P = (95, 41)$
$200P = (77, 77)$	$Q - 200P = (239, 292)$	$220P = (90, 8)$	$Q - 220P = (298, 312)$
$240P = (225, 266)$	$Q - 240P = (31, 9)$	$260P = (213, 327)$	$Q - 260P = (32, 134)$
$280P = (263, 185)$	$Q - 280P = (247, 281)$	$300P = (224, 115)$	$Q - 300P = (50, 201)$
$320P = (192, 327)$	$Q - 320P = (253, 264)$	$340P = (268, 48)$	$Q - 340P = (203, 256)$
$360P = (48, 13)$	$Q - 360P = (318, 125)$	$380P = (286, 165)$	$Q - 380P = (14, 159)$

Notice then that

$$Q - 280P = 3P = (247, 281)$$

Therefore, we conclude that $Q = 283P$ and $k = 283$.

7.4.3. Pollard's Rho Method. Whereas BSGS is very straight-forward since it is based on the division algorithm, Pollard's ρ method (PRM) takes a more "random" approach by using a function f to send a point P_0 through a series of random steps that takes it throughout the group $E(\mathbb{F}_q)$. However, since the group is finite, then f will find a repeat at some point, and f is periodic.

Suppose that we have an initial point $P_0 \in E(\mathbb{F}_q)$. For some randomizing function f, we define P_i recursively by

$$P_{i+1} = f(P_i).$$

If we have two points P_i and P_j with $j > i$ such that

$$P_i = P_j,$$

for smallest possible j for which this holds true, then period d of f is $j - i$ and $P_{i+l} = P_{j+l}$ for all $l \geq 0$.

Suppose that we are given P, Q in $E(\mathbb{F}_q)$ such that $Q = kP$ and we want to find k. Choose random integers $a_0,\ b_0$ and define an initial point P_0 by

$$P_0 = a_0 P + b_0 Q.$$

Partition $E(\mathbb{F}_q)$ into disjoint subsets $S_1, S_2, \ldots, S_s$ so that for each S_i, choose random integers $a_i,\ b_i$, and define a point M_i by

$$M_i = a_i P + b_i Q.$$

Define a function f such that

$$P_{k+1} = f(P_k) = P_k + M_i, \quad \text{if} \quad P_k \in S_i.$$

Write P_{k+1} in terms of P and Q. For $P_k = a_k P + b_k Q$ and $M_i = a_i P + b_i Q$, then

$$P_{k+1} = a_k P + b_k Q + a_i P + b_i Q = (a_k + a_i)P + (b_k + b_i)Q = a_{k+1}P + b_{k+1}Q.$$

When there is a match, say $P_i = P_j$ for $P_i = a_i P + b_i Q$ and $P_j = a_j P + b_j Q$, then we conclude

$$a_i P + b_i Q = a_j P + b_j Q \Rightarrow (a_i - a_j)P = (b_j - b_i)Q.$$

Since $Q = kP$, then for $N = \#E(\mathbb{F}_q)$ if $\gcd(b_j - b_i, N) = 1$, then

$$k = (a_i - a_j)(b_j - b_i)^{-1} \pmod{N}.$$

If for period d, $\gcd(b_j - b_i, N) = d$ then

$$k = (a_i - a_j)(b_j - b_i)^{-1} \pmod{N/d}.$$

7.4.4. PRM Example. Suppose elliptic curve E is given by

$$y^2 = x^3 + 3x - 13 \pmod{331}.$$

Suppose also that points $P = (2, 1)$ and $Q = (300, 227)$ which satisfy E are related such that $Q = kP$ for some integer k. Find k.

By selecting random coefficients as described above, define points $P_0,\ M_0,\ M_1,\ M_2,$ $M_3,\ M_4$ by

$$\begin{aligned}
P_0 &= 3P + 13Q = (247, 281) + (253, 67) = (294, 292) \\
M_0 &= 11P + 17Q = (22, 42) + (260, 233) = (220, 55) \\
M_1 &= 17P + 9Q = (50, 130) + (104, 184) = (178, 73) \\
M_2 &= 18P + 7Q = (272, 225) + (129, 39) = (41, 50) \\
M_3 &= 10P + 9Q = (329, 142) + (104, 184) = (131, 205) \\
M_4 &= 8P + 2Q = (132, 35) + (239, 292) = (241, 127)
\end{aligned}$$

For $P_i = (x_i, y_i)$ if $x_i \equiv k \pmod 5$, then define function f by

$$P_{i+1} = f(P_i) = P_i + M_k.$$

For example, in the first iteration, for $P_0 = (x_0, y_0)$, then $x_0 = 294 \equiv 4 \pmod 5$, thus $M_{k=4}$ will be chosen.

Next, the first few lines of iteration are shown in more depth to show the addition of points and keeping track of the cumulative sums of coefficients of P and Q.

$$\begin{aligned}
P_1 = f(P_0) &= P_0 + M_4 = (294, 292) + (241, 127) = (35, 277) \\
&= (3P + 13Q) + (8P + 2Q) = 11P + 15Q \\
P_2 = f(P_1) &= P_1 + M_0 = (35, 277) + (220, 55) = (329, 142) \\
&= (11P + 15Q) + (11P + 17Q) = 22P + 32Q \\
P_3 = f(P_2) &= P_2 + M_4 = (329, 142) + (241, 127) = (215, 231) \\
&= (22P + 32Q) + (8P + 2Q) = 30P + 34Q \\
P_4 = f(P_3) &= P_3 + M_0 = (215, 231) + (220, 55) = (195, 58) \\
&= (30P + 34Q) + (11P + 17Q) = 41P + 51Q \\
P_5 = f(P_4) &= P_4 + M_0 = (195, 58) + (220, 58) = (41, 281) \\
&= (41P + 51Q) + (11P + 17Q) = 52P + 68Q
\end{aligned} \tag{7.1}$$

The Table 7.3 shows the rest of the iterations with less computation. The reader can verify.

Table 7.3: Iterations of Pollard's Rho Method

$P_6 = (292, 88) = 69P + 77Q$	$P_7 = (178, 73) = 87P + 84Q$
$P_8 = (302, 233) = 97P + 93Q$	$P_9 = (257, 4) = 115P + 100Q$
$P_{10} = (245, 67) = 133P + 107Q$	$P_{11} = (211, 42) = 144P + 124Q$
$P_{12} = (52, 260) = 161P + 133Q$	$P_{13} = (28, 138) = 179P + 140Q$
$P_{14} = (144, 320) = 189P + 149Q$	$P_{15} = (236, 235) = 197P + 151Q$
$P_{16} = (72, 166) = 214P + 160Q$	$P_{17} = (294, 39) = 232P + 167Q$
$P_{18} = (245, 67) = 240P + 169Q$	

We see that $P_{10} = P_{18}$, thus $133P + 107Q = 240P + 169Q$. We have previously shown in § 4.6 that the order of this particular curve is $N = 335$. Then

$$-62Q = 273Q = 107P \pmod{335}.$$

Since $273^{-1} \equiv 27 \pmod{335}$, then $Q = 27 \cdot 107P = 209P \pmod{335}$ and we find

$$k = 209.$$

7.4.5. Notes on PRM. PRM gets its name from the "shape" that the randomness represents. Since f is periodic, it can be thought of as circling in on itself after some initial sequence that is not repeated. Thus the tail of the initial sequence and the circle of the period can form a "p," or the Greek letter ρ, hence the name.

The periodicity of f gives PRM an advantage of BSGS in that, even though both have about the same number of steps in computation, PRM doesn't require the storage of $\sqrt{N}$ that BSGS requires. The function f can be used as a doubling function. Consider the pair of points $[P_i, P_{2i}]$. Then a subsequent pair of points can be found by iterating f on the first point once and iterating f on the second point twice. That is,

$$[P_{i+1}, P_{2i+2}] = [f(P_i), f(f(P_{2i}))].$$

This allows one to to keep only a pair of points until a match is found. Since $d = j - i$, then $d|(j + l + kd) - (i + l)$ for some lth iteration of f of P_i. Thus, in a programming environment, it would only be necessary to hold on to the current set of pairs until a matched is reach. This eliminates the need to store all the single iterations of f and looking for matches.

From the example above, the following pairs occur.

$$\begin{array}{ll}
(P_1, P_2) = [(35, 277); (329, 241)] & (P_2, P_4) = [(329, 142); (195, 58)] \\
(P_3, P_6) = [(215, 231); (292, 88)] & (P_4, P_8) = [(195, 58); (302, 233)] \\
\vdots & \vdots \\
(P_{15}, P_{30}) = [(236, 235); (144, 320)] & (P_{16}, P_{32}) = [(72, 166); (72, 166)]
\end{array}$$

We see that $P_{16} = P_{32}$. Although, not noted above, the coefficients of P and Q were sufficiently tracked so that the reader can verify $P_{16} = 214P + 160Q = 428P + 284Q = P_{32}$. Collecting terms,

$$-124Q = 211Q = 214P \pmod{335}.$$

Multiply by the inverse, $211^{-1} \equiv 181 \pmod{335}$, then $Q = 214 \cdot 181P = 209P$. Thus we conclude $k = 209$.

7.4.6. Pohlig-Hellman Attack. The Pohlig-Hellman Attack (PHA) uses the Chinese remainder theorem (CRT) to reconstruct k from $Q = kP$ ([20] pp. 141-2).

Suppose after determining $N = \#E(\mathbb{F}_q)$ that the factorization of N is known and N has small primes and

$$N = \prod_{i=1}^{r} p_i^{e_i}.$$

Then the goal is to create a base p_i representation k_i of Q so that

$$k_i = a_0 + a_1 p_i + a_2 p_i^2 + \cdots + a_{e-1} p_1^{e-1} \pmod{p_i^{e_i}}.$$

To obtain coefficients a_k for each p_i, first determine a_0. This is essentially solving an instance of ECDLP, but for a small prime. This instance is solved by storing list of $a_i \frac{N}{p_i} P$ for each $a_1 \in [0, p-1]$. The point $\frac{N}{p_i} Q$ is then compared to the list and a match determines the desired a_i. We want to find the first coefficient a_0 of the base p_i expansion by

$$\frac{N}{p_i} Q = a_0 \frac{N}{p_i} P$$

for some $a_0 \in [0, p-1]$. Next, compute Q_1 by

$$Q_1 = Q - a_0 P.$$

Then determine a_1 by

$$\frac{N}{p_i^2} Q_1 = a_1 \frac{N}{p_i} P$$

for some $a_1 \in [0, p-1]$. (Note here that the denominator p_i does not increase on the right-hand side for P as it did in the left-hand side for Q. This means that it is not necessary to create and store a new list for successive powers of p_i.) Then $Q_2 = Q_1 - a_1 P$ and subsequently, a_2 can be extracted is the same manner as a_0 and a_1. Each a_k is then systematically extracted by increasing the power of p_i up to $e - 1$, and solving ECDLP in each case. Use the extracted a_k from each power of p_i to create a congruence modulus $p_i^{e_1}$. This process is then repeated for each $p_i|N$. Lastly, the system of equations

$$\begin{aligned} k &\equiv k_1 \pmod{p_1^{e_1}} \\ k &\equiv k_2 \pmod{p_2^{e_2}} \\ &\vdots \\ k &\equiv k_r \pmod{p_r^{e_r}} \end{aligned}$$

is solved by CRT to obtain k.

7.4.7. PHA Example.. Given the curve E determined by

$$y^2 = x^3 + 28x + 662 \pmod{701}$$

with $P = (2, 5)$, $Q = (119, 500)$ and the relation $Q = kP$, solve for P.

First, we can verify that $N = \#E(\mathbb{F}_{701}) = 722$, thus $N = 2 \cdot 19^2$. We want to build two congruence equations for modulus 2 and modulus 19^2.

To extract a_0 for $p = 2$, first we determine $\frac{N}{q}P = \frac{722}{2}P = 361P = (689, 0)$. For $361P$, we create a set S_2 of $j(361P)$ for $j \in [0, 1]$. Thus

$$S_2 = \{0(361P) = \infty;\ \ 1(361P) = (689, 0)\}$$

Then we determine $\frac{N}{q}Q = \frac{722}{2}Q = 361Q = \infty$. Thus for $\frac{N}{q}Q = a_0 \frac{N}{q}P$, then we see $a_0 = 0$. Since $p = 2^1$, then no further iterations of the algorithm are necessary. Thus $k_2 = 0 \pmod 2$ and we have the first congruence statement

$$k \equiv 0 \pmod{2}.$$

To extract a_0 for $p = 19$, first we determine $\frac{N}{q}P = \frac{722}{19}P = 38P = (82, 559)$. Table 7.4 shows the j-multiples of $38P$ for $j \in [0, 18]$.

Table 7.4: Multiples of $38P$ for Pohlig-Hellman Attack

$0(38P) = \infty$	$1(38P) = (82, 559)$	$2(38P) = (88, 628)$
$3(38P) = (444, 380)$	$4(38P) = (476, 36)$	$5(38P) = (613, 48)$
$6(38P) = (211, 80)$	$7(38P) = (403, 421)$	$8(38P) = (547, 545)$
$9(38P) = (108, 687)$	$10(38P) = (108, 14)$	$11(38P) = (547, 156)$
$12(38P) = (203, 280)$	$13(38P) = (211, 621)$	$14(38P) = (613, 653)$
$15(38P) = (476, 665)$	$16(38P) = (488, 321)$	$17(38P) = (88, 73)$
$18(38P) = (82, 142)$		

Then we determine $\frac{N}{q}Q = \frac{722}{19}Q = 38Q = (613, 48)$. Thus for $\frac{N}{q}Q = a_0\frac{N}{q}P$, we see that $a_0 = 5$. Since $19^2|N$, the algorithm must iterated again. Let $Q_1 = Q - a_0P = Q - 5P = (119, 500) + (192, -624) = (314, 169)$. We can extract a_1 by $a_1\frac{N}{q}P = \frac{N}{q^2}Q_1 = \frac{722}{361}Q_1 = 2Q_1 = (108, 14)$. Thus $a_1 = 10$. We now build the second congruence statement, $k_{19} = 5 + 10 \cdot 19 \equiv 195 \pmod{19^2}$. And the second congruence equation is

$$k \equiv 195 \pmod{361}.$$

Solving the two equations, we determine that $k = 556$.

7.5. Key Exchange/Encryption

7.5.1. Diffie-Hellman Key Exchange (DHKE). As mentioned earlier, the asymmetric elliptic curve key exchanges allow for the exchange of a private key for a symmetric system. DHKE is one such exchange ([20] pp. 160-1).

Alice and Bob choose an elliptic curve E such that the ECDLP is deemed hard.

They chose a point P on E such that the order of P is a large prime. Then they follow the outlined procedure.

1. Alice chooses her own secret integer a and computes $P_a = aP$ and sends the result to Bob.
2. Bob chooses his own secret integer b and computes $P_b = bP$ and sends the result to Alice.
3. After receiving P_b from Bob, Alice uses her integer a and computes $P_{ab} = aP_b = abP$.
4. After receiving P_a from Alice, Bob uses his integer b and computes $P_{ab} = bP_a = abP$.
5. Alice and Bob use agreed upon method to extract the private key from P_{ab}.

Notice that the elliptic curve E, and points P, aP, and bP, are broadcast. This is the information that Eve will be able to see. Since E is chosen so the ECDLP is considered hard, then Eve should not be able to extract a or b from aP or bP in reasonable time. If she can extract a or b, then she will be able to easily determine P_{ab}. Finding this information is again the essence of ECDHP, which is no harder than the ECDLP.

7.5.2. Massey-Omura Encryption. Asymmetric systems, such as RSA and elliptic curve cryptography, can be used to encode and decode information.

Alice and Bob agree on an elliptic curve E over $\mathbb{F}_q$ where the ECDLP is deemed intractable for $E(\mathbb{F}_q)$. Let $N = \#E(\mathbb{F}_q)$. Then the following steps are used to transmit and decode the message.

1. Let M denotes Alice's message. Alice chooses a secret integer a such that $\gcd(a, N) = 1$ and computes $aM = M_a$ and transmits to Bob.
2. Bob receives M_a from Alice. He then chooses his own secret integer b such that $\gcd(b, N) = 1$ and computes $bM_a = abM$ and sends this to Alice.
3. Alice receives abM from Bob. Since $\gcd(a, N) = 1$, Alice then determines the inverse of her integer a^{-1} computes $a^{-1}abM = bM$ and transmits the result to Bob.
4. Bob has now received bM from Alice. Since $\gcd(b, N) = 1$, Bob then computes the inverse of his integer b^{-1} and computes $b^{-1}bM = M$. Bob now has the original message M.

Notice that Eve will see E, N, M_a, abM, and bM. If Eve can extract b from abM, then she can determine $b^{-1} \pmod{N}$ and can then easily find M by taking $M = b^{-1}bM$. The intractability of the ECDLP in this case will keep M secure.

7.5.3. ElGamal Public Key Encryption. The following steps outline a method in which a sender's public key is broadcast and used to encode and decode messages ([20] pp. 164-5).

1. Alice chooses an elliptic curve E defined over $\mathbb{F}_q$ such that the ECDLP for $E(\mathbb{F}_q)$ is deemed to be hard. Alice chooses a point P on E such that the order of P is a large prime. Alice then chooses her own secret integer a and computes $K = aP$. The integer a is Alice's private key. Alice then broadcasts E, $\mathbb{F}_q$, P, and K, all of which are Alice's public key.

2. Bob wants to send a message to Alice. Bob downloads Alice public key information. Bob creates a message M. Bob then chooses a private key b and computes $M_1 = bP$. He also then computes $M_2 = M + bK$. He sends M_1, and M_2 to Alice.

3. Alice receives M_1 and M_2 from Bob. Then Alice takes her private-key a and computes M by

$$M_2 - aM_1 = (M + bK) - a(bP) = M + b(aP) - b(aP) = M.$$

We notice that Eve knows E, $\mathbb{F}_q$, P, K, M_1 and M_2. If Eve is able to extract a from $K = aP$, then M comes easily from M_1 and M_2. The intractability of the ECDLP in this case will keep Alice's private key secure and M safe.

7.6. Digital Signatures

Digital signatures are used to show that a message originated from a legitimate source, that is, Eve is unable to send new messages having disguised herself as being Alice or Bob. If a signature scheme prevents Eve from generating valid signatures of new messages, then the scheme is said to be secure as defined by Goldwasser, Micali, and Rivest (called GMR-secure). The definition of GMR-secure signature schemes is strong in the sense that it assumes that Eve has exceptional capabilities yet has only the intention of signing any new message, useless or not. This definition has gained wide acceptance as being the correct mentality towards signature schemes. Just as we explored one particular RSA digital signature algorithm, there are digital signature algorithms for elliptic curves analogous to the one described for RSA.

7.7. The Elliptic Curve Cryptography (ECC) Advantage

Although the theory of elliptic curve cryptography deals with the mathematics, the actual implementation of such systems requires the use of physical systems where such considerations as power consumption, storage, running time of algorithms, number of processors used and their speeds, available bandwidth, and other considerations. Not all algorithms are the same, and there is no one standard to measure the efficiency of an algorithm. Different applications require different algorithms and security companies vary in their available resources to execute various algorithms.

The three different cryptosystems (RSA, DL, and ECC) all lend their security to the hardness of their respective problems: RSA to the integer factorization problem, DL systems to DLP, and EC systems to the ECDLP. The perceived hardness affects the size of the parameters of the domains of the systems so that the problems remain intractable within reasonable time. The size of the parameters in turn affects the speed and resources necessary to carry out such systems.

The short answer is that EC systems are advantageous in that fewer bits are required to run them. Washington states that the hardness of solving ECDLP in a 313-bit instance of an EC system is comparable to solving DLP in a 4096-bit instance in a RSA system ([20] p. 159). Likewise, Hankerson et al. state that solving ECDLP in 256-bit instance of an EC system is comparable to solving DLP in a 3072-bit instance of integer factorization ([8] p. 196). The number of bits for EC systems to be secure compared to another system from the same attack can be up to a factor of 30 in some cases. Fewer bits require less storage, and less processing time, thus making EC systems faster and less costly overall.

8. CONCLUSION

Elliptic curves have certainly pushed the boundaries of mathematics and broadened our understanding of numerous fields simultaneously. Studying elliptic curves requires studies in fields such as complex analysis, abstract algebra, cyclotomic fields, matrix theory, and algebraic geometry, just to name a few. Certainly the author's understanding of mathematics as a whole has been broadened by this study.

This thesis has mentioned two of the Millennial problems and Fermat's Last Theorem. It is interesting to note how these problems are related to elliptic curves. Also note that the Birch-Swinnerton-Dyer conjecture that deals directly with elliptic curves also uses a function related to the one arising in the Riemann hypothesis. So a solution to the Riemann hypothesis may require a journey through elliptic curves.

Certainly, the expansion of knowledge in the area of elliptic curves will fuel further insights to all of mathematics.

REFERENCES

[1] C. Bach, Online elliptic curve calculator, available for free at http://christelbach.com/ECCalculator.aspx.

[2] E. Brown, Three Fermat trails to elliptic curves, Col. Math. J. 31 (2000) 162–172, https://www.jstor.org/stable/2687483.

[3] D.A. Cox, Introduction to Fermat's last theorem, Am. Math. Monthly 101 (1994) 3–14, https://www.jstor.org/stable/2325116.

[4] L. Crane, Quantum computer sets new record for finding prime number factors, available for free with subscription at https://www.newscientist.com/article/2227387-quantum-computer-sets-new-record-for-finding-prime-number-factors/.

[5] F. Doménech, Fermat and the greatest problem in the history of mathematics, available at http://www.bbvaopenmind.com/en/science/leading-figures/fermat-and-the-greatest-problem-in-the-history-of-mathematics/.

[6] A. Dujella, Rank $\geq$ 28, available at http://web.math.pmf.unizg.hr/~duje/tors/rk28.html.

[7] S.L. Garrett, On the Quadratic Sieve, available at http://libres.uncg.edu/ir/uncg/f/umi-uncg-1581.pdf.

[8] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, New York, 2013.

[9] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, vol. 52, Springer, New York, 1977.

[10] T. Hungerford, Abstract Algebra: An Introduction, 3rd ed., Cengage Learning, Delhi, 2013.

[11] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, 2nd ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.

[12] L. Lienau, A brief history of perspective, available at http://www.classicalart.org/blog/a-brief-history-of-perspective.

[13] S. Nakov, RSA signatures, available at http://cryptobook.nakov.com/digital-signatures/rsa-signatures.

[14] K.A. Ribet, From the Taniyama-Shimura conjecture to Fermat's last theorem, Annales de la Faculté des Sciences de l' Université de Toulouse 11 (1990) 116–139, https://math.berkeley.edu/∼ ribet/Articles/toulousela.pdf.

[15] A. Rice, E. Brown, Why ellipses are not elliptic curves, Math. Mag. 85 (2012) 163–176, https://www.jstor.org/stable/10.4169/math.mag.85.3.163.

[16] K.H. Rosen, Elementary Number Theory and its Applications, 5th ed., Addison-Wesley, Boston, 2005.

[17] J.H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009.

[18] J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves, 2nd ed., Undergraduate Texts in Mathematics, Springer, New York, 2015.

[19] T.V. Venkateswaran, When Ramanujan did mathemagic with a taxi number, available at http://thefederal.com/features/when-ramanujan-did-mathemagic-with-a-taxi-number/.

[20] L.C. Washington, Elliptic Curves: Number Theory and Cryptography, Discrete Mathematics and Its Applications, Ed. K.H. Rosen, CRC Press, Boca Raton, FL, 2003.

[21] Wikipedia, Enigma machine, available at
http://en.wikipedia.org/wiki/Enigma_machine.

[22] Wikipedia, Lenstra elliptic curve factorization, available at
http://en.wikipedia.org/wiki/Lenstra_elliptic-curve_factorization.

[23] Wikipedia, Mathematics and art, available at
http://en.wikipedia.org/wiki/Mathematics_and_art.

[24] Wikipedia, Modularity theorem, available at
http://en.wikipedia.org/wiki/Modularity_theorem.

[25] Wikipedia, Primality test, available at http://en.wikipedia.org/wiki/Primality_test.

[26] Wikipedia, RSA numbers, available at http://en.wikipedia.org/wiki/RSA_numbers.

[27] Wikipedia, Taxicab number, available at https://en.wikipedia.org/wiki/Taxicab_number.