A Classroom Exercise: Elliptic Curves

Ben Aron[†]

[†]Department of Mathematics
Temple University

April 29th, 2022

1 Introduction

In this paper, we give a brief introduction to elliptic curves and some basic properties. This paper was written for the course *MATH 3101 Topics in Modern Algebra* taught by Dr. Matthew Stover in which rings, vector spaces, fields and Galois theory were covered. Undoubtedly, elliptic curves is a subject that has been deeply covered and explored in mathematics and this paper may perhaps seem pedantic. However, the point of this paper is to give my classmates and perhaps other students in the undergraduate curriculum, a window into a fascinating and rich topic.

We begin with a brief history of elliptic curves, why they are interesting and how they were developed. We continue with an introduction to cubic curves as well as constructions on them. Following this, we explore the Group Law, Mordell's theorem and an introduction to elliptic curves. Finally, we discuss applications and some constructions. Throughout this paper, we also include examples in which we made with Mathematica. Please see the code attached for reference.

2 A Brief History of Elliptic Curves

The early history of elliptic curves is unsurprisingly overlapped with the history of many other ideas and subjects. The theory of elliptic curves spans several topics including number theory, analytic geometry, algebraic geometry, automorphic and modular forms, and noncommutative harmonic analysis, to name a few. One of the first major players in our story of elliptic curves was Diophantus of Alexandria. Diophantus' major work was the *Arithmetica*, a treatise on algebra and number theory. In particular, it contains numerical solutions of determinate and indeterminate polynomial equations. Like many ancient texts, a good portion of it has been lost. Moreover, during the Dark Ages and beyond, the *Arithmetica* was known to few. It was only until it was translated into Latin, by Bachet and others, did the

text become widely known.

It was Bachet who ultimately laid the foundation for further discovery. In 1621, he discovered what is known as Bachet's duplication formula which produces rational solutions to Bachet's equation- more on this later. One of the translation's avid readers was none other than Pierre de Fermat. In fact, it was in the margin of this translation that Fermat wrote his famous Last Theorem. This and his other work ignited mathematics' study of Diophantine equations, and so the subject of elliptic curves was born. The rest of the historical background, that is, post-Fermat, will be sprinkled throughout the rest of the paper.

3 Cubic Curves

A general cubic curve of two variables is a somewhat not so pretty object. The definition of a general cubic polynomial in two variables is given as follows:

Definition 1 (Cubic Polynomial)**.** A *cubic polynomial in two variables* is a polynomial of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0. \tag{1}$$

We say that Eq. (1) is a *rational cubic* if the coefficients above are rationals.

Instead of dealing with this generalized cubic, let us first focus on a much simpler form, that which is known as Bachet's equation. This is a Diophantine equation, i.e., a polynomial equation which has solutions in either the integers or the rationals. Bachet's equation is given by

$$y^2 - x^3 = c, \tag{2}$$

where c is some fixed integer. This is an equation in which we are concerned with its rational and integer solutions. In fact, Bachet showed that if you have a rational solution, (x, y) for this equation, then for $y \neq 0$, we can obtain another rational solution. The means in which this is possible is through what is known as Bachet's duplication formula, given by,

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right). \tag{3}$$

We plot Bachet's equation in Fig. 1 and proceed by proving the duplication formula for this equation.

Proposition 1. Given Bachet's equation, $y^2 - x^3 = c$, for $c \in \mathbb{Z}$ and rational solutions x, y with $y \neq 0$, there exists another rational solution given by the formula,

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right). \tag{4}$$

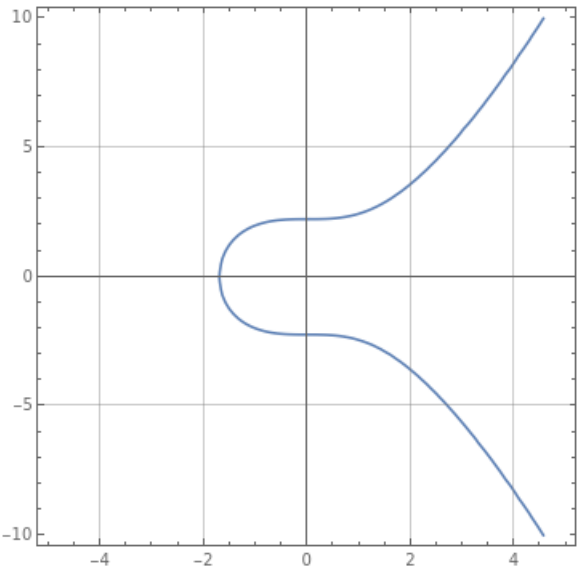

Figure 1: Bachet's Equation for a given c.

Proof. Given Bachet's equation at the rational point (x_1, y_1), we may implicitly differentiate both sides to get

$$\begin{aligned} &\frac{d}{dx_1}(y_1^2 - x_1^3) = \frac{d}{dx_1}(c) \\ \implies &\frac{d}{dy_1}(y_1^2)\frac{dy_1}{dx_1} - 3x_1^2 = 0 \\ \implies &\frac{dy_1}{dx_1} = \frac{3x_1^2}{2y_1}. \end{aligned} \tag{5}$$

We note that this is the slope of the tangent line $y_1 = mx_1 + b$ at the rational point (x_1, y_1). Then plugging in for the slope, we obtain,

$$\begin{aligned} y_1 &= \frac{3x_1^2}{2y_1}x_1 + b \\ \implies b &= y - \frac{3x_1^2}{2y_1} \\ \implies b &= \frac{2y_1^2 - 3x_1^2}{2y_1}. \end{aligned} \tag{6}$$

Then this line given by $y = mx + b$ tangent to the point (x_1, y_1) intersects with the curve $y^2 - x^3 = c$. Thus we obtain a cubic equation of a single variable given by

$$(mx + b)^2 = c + x^3 \implies x^3 - m^2x^2 - 2bmx + b^2 - c = 0. \tag{7}$$

We already know that Eq. (7) given above is satisfied for $x = x_1$ since the line and curve intersect at (x_1, y_1) as we have constructed. Further, as we have learned in class, the cubic polynomial in Eq. (7) has at most 3 distinct roots over $\mathbb{Q}$. We will now invoke a lemma in which we leave as an exercise to prove:

Lemma 1. Given any real point, P, satisfied by Bachet's equation, $y^2 - x^3 = c$, we can construct a tangent line to P (as was done in Eq. (6)) that will intersect the curve in at most one other point. This is illustrated in Fig. 2.

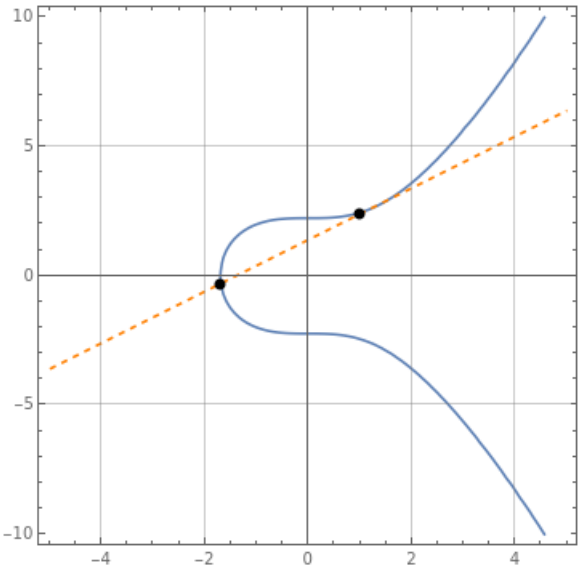

Figure 2: Illustration of Lemma 1.

Given Lemma 1 above, we will notice that two of the roots for the polynomial given in Eq. (7) occur at the point (x_1, y_1). That is, $x = x_1$ is twice a root (i.e., has multiplicity 2) of the polynomial given in Eq. (7). Now, we know that the third root, as given by Lemma 1, will occur at another point, say (x_2, y_2). Thus, $x = x_2$ is our third root. We now require one last lemma to finish our proof.

Lemma 2 (Vieta's formula for cubic polynomials of a single variable)**.** Given the polynomial $f(x) = ax^3 + bx^2 + cx + d$, if the equation $f(x) = 0$ has roots r_1, r_2, r_3, then $r_1 + r_2 + r_3 = \frac{-b}{a}$.

Sketch of Proof. Use factor theorem. □

Now, applying Lemma 2 to Eq. (7) gives us

$$x_1 + x_1 + x_2 = m^2 \implies 2x_1 + x_2 = m^2. \tag{8}$$

Solving for x_2 now implies that $x_2 = m^2 - 2x_1$. Plugging in for m and using algebra, we obtain

$$x_2 = \frac{x_1^4 - 8cx_1}{4y_1^2}. \tag{9}$$

Then we can easily get y_2 by using the fact that $y_2 = mx_2 + b$, where m, b and x_2 are now given. This gives

$$y_2 = \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}. \tag{10}$$

Hence, we obtain Bachet's duplication formula, as desired. □

Moreover, Bachet's duplication formula gives us a set of infinitely many rational solutions except when $c = 1$ or -432.

Now, for general Diophantine equations, for say of two variables, that we notate as $f(x, y)$, we can ask similar questions about their properties to see what we can deduce about them. Do we obtain a duplication formula for rational points on general Diophantine equations of two variables? If a duplication formula exists, do we obtain infinitely many solutions in rationals? Integers? These are the questions that are generally asked when first talking about Diophantine equations. However, we will focus on cubic equations. Our main concern with cubic equations is being able to find rational or integer solutions to them. This brings us to the following definition:

Definition 2 (Cubic Curves)**.** A *cubic curve* is the graph of the real solutions of a polynomial with degree 3 in the $xy-$plane.

For example, our Bachet equation that we plotted in Fig. 1 is a cubic curve.

4 Constructions on Cubic Curves

We have seen previously that we can obtain rational solutions on a cubic curve. Now we turn our attention to rational lines.

Definition 3. A line is *rational* if the equation of the line can be written as

$$ax + by + c = 0, \tag{11}$$

where a, b and c are rational numbers.

We already saw that if we have one rational solution, we can generally obtain another from devising a duplication formula as we did with Bachet's equation. This is of course, easier said than done, but given any rational cubic, that is a cubic with rational coefficients, we can draw a tangent line to the rational point and obtain another point that will be rational.

Now, we may ask, can we do this without using a tangent? That is, can we obtain a rational point on a rational cubic by just intersecting a line through another point? We will see that indeed we can, but there is need for a clarification. Lines can be constructed if we have two points already known. That is, in order to obtain another rational point, we need to already know two rational points. In this way, we can construct a line that passes through these two rational points and perhaps get a third point. How do we know that the third point is rational? Since both the line and the cubic are rational, when we intersect them, that is, by setting them equal to each other, we find that we obtain a rational cubic polynomial of one variable. Now, we already know that two points, i.e., two intersection points are rational so the third root for the cubic equation obtained from intersection is also rational. That is, the third intersection point is rational. This can be proved using Lemma 2.

This was a long way of saying the following:

Proposition 2. If we have two rational points, P and Q, we can draw a line through P and Q to obtain a third rational point labelled as $P * Q$.

This is not so trivial to prove generally. Instead, it can be proven for much simpler rational cubics like Bachet's equation. In fact, Bachet's equation is a special case of Proposition 2 as explained in the following Corollary.

Corollary 1. Given one rational point P on a rational cubic, we can draw a tangent line to this cubic at P to obtain a second rational point, $P * P$.

We will note that the first and second intersections are given by P and again by P. This is similar to what we had proving Proposition 1 where we obtained a double root. Proposition 2 and Corollary 1 are shown for Bachet's equation in Fig. 3. As can be seen in Fig. 3 and

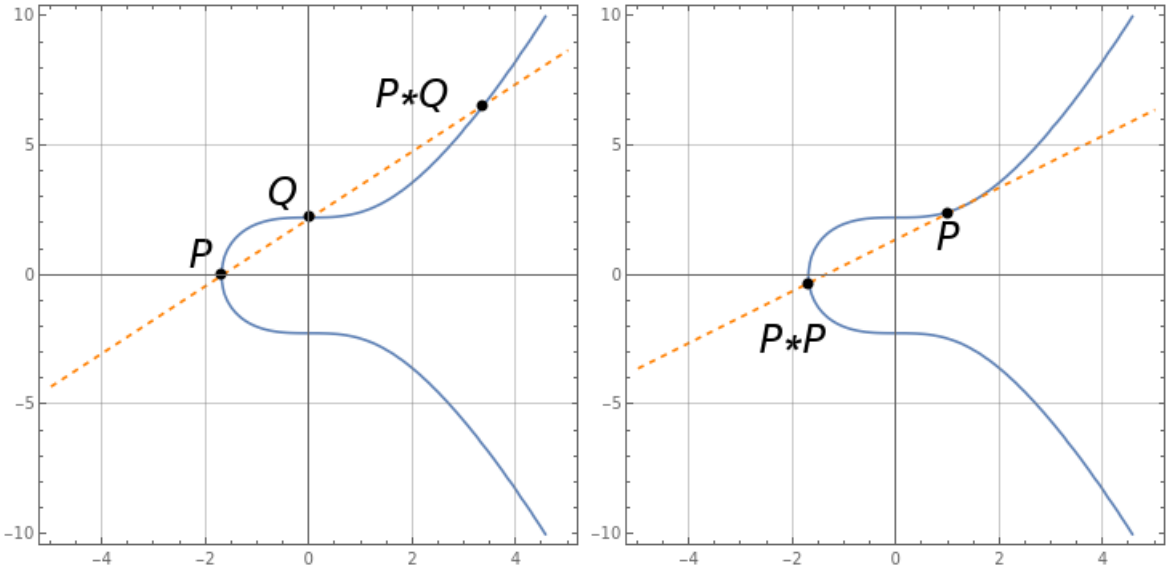

Figure 3: Illustrations of Proposition 2 and Corollary 1

Proposition 2, we have constructed both an algebraic and geometric operation. One can now ask a myriad of questions about the algebraic and geometric structure of what we have constructed. For instance, can we construct a group using this operation along with some set of rational points?

5 The Group Law

To answer the above question, we do not obtain a group. However, it is clear that we can construct a magma- the rational lines that we can construct on our rational cubic clearly intersect at rational points by construction. That is, the points that intersection points of our rational line and rational cubic are again rational. This is a trivial, yet useful exercise into exploring the algebraic properties of our operation and the set of rational solutions to a given cubic. In fact, one can obtain a group by adding an identity element to our set and adding an operation. This operation is defined by the following proposition:

Proposition 3. Given a fixed rational point on a given cubic that we label as O, we define the operation, '+' as following:

$$P + Q = O * (P * Q), \tag{12}$$

where P and Q are known rational points, and O is the identity element.

Proof. We begin by proving that this operation makes sense, i.e., that it is closed. To do this, we will use Proposition 2. Given P and Q, we form a line and obtain the third point of intersection $P * Q$ by Proposition 2. Now, given the rational point O and $P * Q$, we form a line and obtain a third point of intersection, $O * (P * Q)$, by Proposition 2, as desired. Now, labelling this as $P + Q$ is just notation. This is illustrated in Fig. 4 for Bachet's equation.

We will now show that O is indeed the identity. Given known rational points P and O, we may apply Proposition 2, to obtain the third point $O * P$. Then using the closure as above, we know that $P + O = O * (P * O)$. But we know each intersection point: O, P and $O * P$. Thus $O * (P * O)$ must be P. That is, $P + O = P$. Therefore, O is the identity element for our operation '+'. This is illustrated in Fig. 5 for Bachet's equation. □

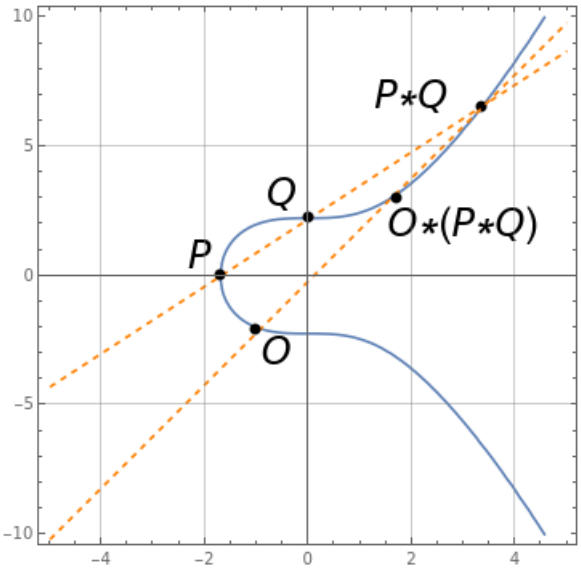

Figure 4: Illustration of Proposition 3.

Given the operation defined in Eq. (12), we can indeed obtain a group.

Proposition 4. The set of rational points on a given cubic along with the operation '+' defined in Eq. (12) is an abelian group.

Sketch of Proof. Use Proposition 2 and 3 to prove associativity and existence of inverses. Closure and existence of the identity element were proved in Proposition 3. □

Now that we have constructed a group, we can use what we know from modern algebra to play around with it. That is, we can form maps and even isomorphisms. We can even say something about generating the group of rational points. This leads us to Mordell's Theorem.

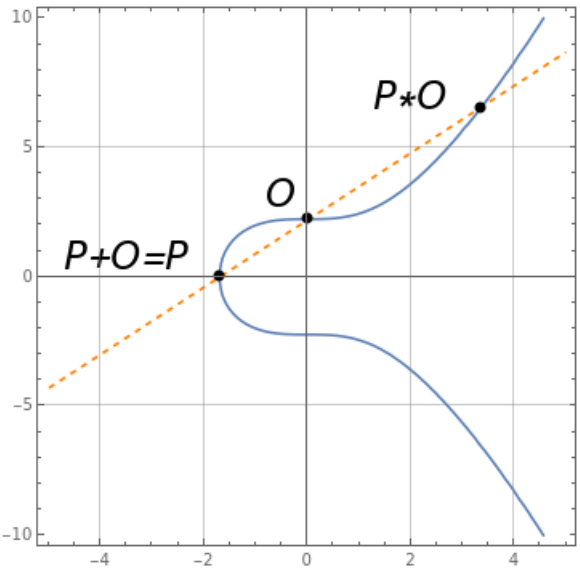

Figure 5: Visual proof that O is indeed the identity element.

6 Mordell's Theorem

Before we write down Mordell's Theorem, there is need for some definitions.

Definition 4. A *cubic plane curve* is the zero set of a cubic polynomial in two variables, i.e., the set of all solutions to the equation

$$f(x, y) = 0, \tag{13}$$

where $f(x, y)$ is a given cubic.

We will realize that Definition 4 is just a reformulation of Definition 2. For our purposes, we will consider rational cubic curves as was discussed in Section 4.

Definition 5. A *non-singular rational cubic plane curve* is a rational cubic curve of the form $f(x, y)$ that does not have any points such that the partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish simultaneously.

We can now state Mordell's Theorem.

Theorem 1 (Mordell's Theorem)**.** If a non-singular rational cubic plane curve has a rational point, then the group of rational points as defined in Proposition 4 is finitely generated.

The proof of this theorem is beyond the scope of our purposes, but we will explain how to develop a proof as Mordell did in 1922. Mordell's theorem essentially says that if we are given a particular finite set of rational points on a cubic curve, all other rational points on that curve can be obtained by repeated addition as we defined in Proposition 3.

The proof of Mordell's theorem uses rational cubic curves that are transformed into a form that is easier to deal with. That is, if any cubic curve has a rational point, then it can

be transformed into what is known as *Weierstrass normal form.* Equations of this form look like

$$y^2 = x^3 + ax^2 + bx + c, \tag{14}$$

where a, b and c are rational numbers. We will notice that Bachet's equation is of this form. In fact, using cubic curves in Weierstrass normal form leads us to the definition of elliptic curves.

7 Elliptic Curves

Definition 6 (Elliptic Curve)**.** An *elliptic curve* is a non-singular rational cubic plane curve that is in Weierstrass normal form.

For example, Bachet's equation as given in Eq. (2) is an elliptic curve. We will realize that what makes elliptic curves special is not only the cubic form, but also the non-singularity of the curve. We defined earlier that non-singularity just means that the partial derivatives do not vanish simultaneously. Put in a more geometric way, the curve has no self-intersections or vertices.

Now, given an elliptic curve, we can ask the same questions about adding points on cubic curves. We saw before that we can essentially add any rational point to the list of rational points that we previously obtained. In practice, this is just applying Mordell's Theorem. We can do the same for elliptic curves. However, there is now need for a clarification of where the identity element O is. In Fig. 4, we fixed O to be some rational point on the given cubic. But, we neglected to say that this curve is an elliptic curve since we had not defined it yet. That is, the identity element on an elliptic curve has a unique definition. Not going into projective geometry will require us to accept that there exists a rational point at infinity. We will take it on faith that this is the case. Note that it is projective geometry that allows us to say that parallel lines intersect at infinity. Therefore, we set the identity element O to be our rational point at infinity. We can now redefine our rule for adding rational points to our set of known rational points.

Proposition 5. For given rational points P and Q, we use Proposition 2 to find $P * Q$. Then the operation '+' is given as a reflection of the point $P * Q$ across the x-axis.

Proof. As in Proposition 3, the operation '+' is given by Eq. (12). Then $O * (P * Q)$ is given as the line adjoined by the points O and $P * Q$. Since O is a point at infinity, the line will be a vertical line passing through the point $P * Q$. Thus, our third point of intersection will be the intersection of a vertical line passing through the point $P * Q$ and the elliptic curve, given by $P + Q$. Then we note that all elliptic curves are symmetric about the x-axis (left as an exercise). Therefore, the point $P + Q$ is given as a reflection of the point $P * Q$ about the x-axis. □

Proposition 5 is a very nice way of getting additional rational points. It also makes proving Proposition 4 much easier since we can easily find inverses by reflecting points about the x-axis. We illustrate Proposition 5 in Fig. 6.

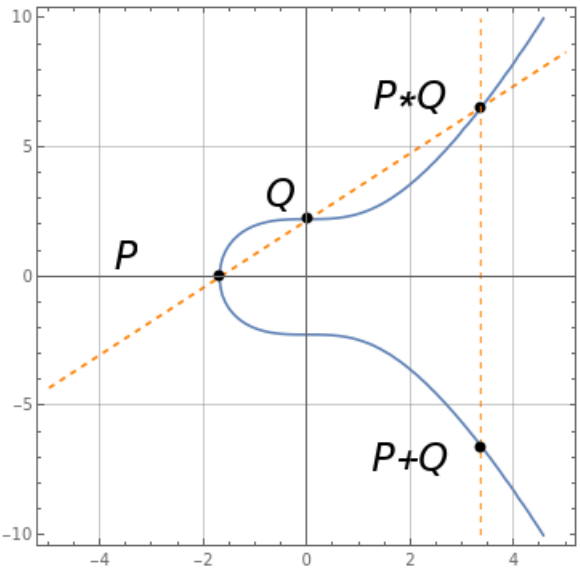

Figure 6: Illustration of Proposition 5 for Bachet's equation with a given c.

8 Applications of Elliptic Curves

We will now focus on applications of elliptic curves. As with many ideas in mathematics, there are many applications that we can explore. One such application is in factoring. The Fundamental Theorem of Arithmetic tells us that any positive integer can be factored uniquely as a product of primes. However, actually performing the factoring for large numbers can be virtually impossible. Enter elliptic curves. It was in 1987 that Hendrik Lenstra built an algorithm using elliptic curves that factors large integers efficiently. However, the elliptic curves that are used are of a somewhat different variety. Instead of defining an elliptic curve over the real numbers, we can actually define an elliptic curve over any finite field. For more on this, please refer to Silverman and Tate's *Rational Points on Elliptic Curves*, the main text used to write this paper.

Once we understand elliptic curves defined over finite fields, we can define the algorithm needed to factor large integers. The algorithm chooses a random elliptic curve over the finite field $\mathbb{Z}/n\mathbb{Z}$, where n is prime. Then by repeatedly adding points as we have done so for elliptic curves over the reals, we can factor our integer by taking the modulo n of $P + ... + P$. If this does not produce a factorization, the algorithm is repeated for a different elliptic curve.

This then brings us to another application of elliptic curves- that of Elliptic Curve Cryptography or ECC. This is an approach to the public-key cryptography using elliptic curves, i.e., encryption using elliptic curves. Without going into public-key encryption ideas, we can simply say that ECC is a more secure method than other public-key encryption methods like RSA since it relies on more complicated ideas like factoring integers by means of random elliptic curves. Of course, the invention of quantum computers would render all of these methods obsolete.

The last application that we will explore is to Fermat's Last Theorem. In a way, Fermat is partly to blame for the study of elliptic curves and so we suppose it is apt that elliptic

curves were used to prove his Last Theorem. Without going into the details, elliptic curves were used by Andrew Wiles to prove the fact that for integers, n, strictly greater than 2, there are no solutions to the equation $x^n + y^n = z^n$, for x, y and z. The proof by Andrew Wiles used modular forms and other complex ideas that rely on elliptic curves. The extent of applications that elliptic curves provides is clearly vast and useful. However, for our purposes, we can use the elliptic curves that we defined to procure simple constructions.

9 Constructions on Elliptic Curves

In this section, I will explore other possible ways of constructing rational points on elliptic curves given that we know the rational points P and Q by using a straightedge and compass. Suppose that P has rational coordinates (x_1, y_1) and Q has rational coordinates (x_2, y_2). Then we say that the third point of intersection, $P * Q$ has rational coordinates (x_3, y_3). Then we will note that any rational number that we subtract from $P * Q$ will again be rational. That is, the rational line formed between the points P and $P * Q$ has a rational distance since we find the distance from subtracting points. Thus, we can subtract half this distance to get half of the distance between P and $P * Q$. We note that WLOG we perform this operation when Q is between P and $P * Q$, as in Fig. 3.

Thus, we can obtain a midpoint between P and $P * Q$. This is explicitly given by the formula

$$R = \frac{1}{2}(P * Q - P) = \frac{1}{2}(x_3 - x_1, y_3 - y_1) = \left(\frac{x_3 - x_1}{2}, \frac{y_3 - y_1}{2}\right). \tag{15}$$

We call this midpoint R. Then taking our compass, we can draw the circle with center R and radius RP or $R(P * Q)$. This is shown in Fig. 7. We will call this circle rational. This leads us to the following question: Can we obtain another rational point on the elliptic

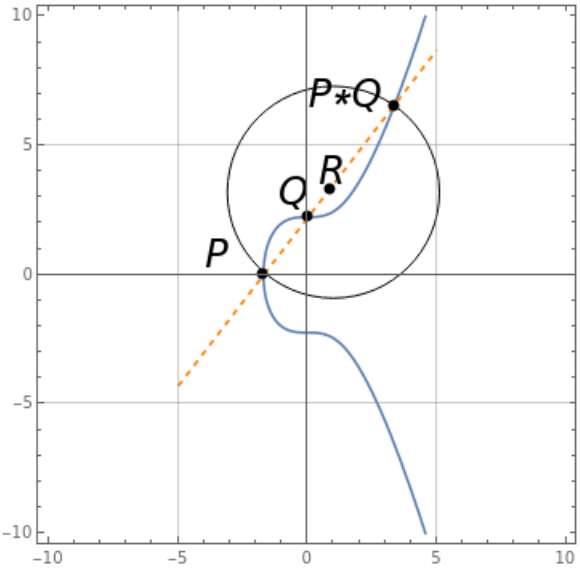

Figure 7: Drawing a rational circle on our elliptic curve.

curve by intersecting it with a rational circle? As can be seen in Fig. 7, the circle does not

even intersect the curve again so asking this question for what we constructed in Fig. 7 is irrelevant.

Now, we can also add another construction to what we already have in Fig. 7. Suppose we take our compass and create two circles of radius RP and $R(P * Q)$ centered at P and $P * Q$, respectively. Then as we had in class, we obtain a point that is intersected by the two circles. Now our question becomes, can we continue this process of creating rational circles with rational radii to intersect the elliptic curve and obtain a rational point? Furthermore, can we construct other objects such as regular polygons using intersections of points from one or several rational lines adjoining rational points on our elliptic curve? We can also ask that if we can create points on our elliptic curve that form a polygon, how many of those vertices on it will be rational?

10 Discussion

Elliptic curves encompass an immense amount of information and subjects that exploring even the basics becomes daunting. We are hopeful that this paper gives a brief outline of where and how to begin studying elliptic curves. Supposing you know a few things, further exploration into elliptic curves can be accomplished with diligence and a keen interest.

As we have seen in Section 8 and 9, once we have built up and defined elliptic curves, we can endlessly explore their properties and applications. Continuing on these ideas, we believe the next ideas to explore are the questions posed in Section 9. What can we construct using a straightedge and compass on rational lines formed by adjoining rational points on cubics? There are of course two main approaches in trying to understand this: the first is geometrically as we have done so in Fig. 7 and the second is from an algebraic perspective. Of course, the two are undoubtedly intertwined but as far as intuition, the geometric constructions may be the way to go. We do hope, however, that these questions and others asked by the reader inspires for further exploration and study of this subject. Thanks to Dr. Matthew Stover for inspiring the idea for this paper and for sending along some interesting materials.

11 Appendix

Listed below is the Mathematica code we used to create the figures above.

Mathematica Code

```
c1=ContourPlot[y^2-x^3==5,{x,-5,5},{y,-10,10},
    GridLines->Automatic,Axes-> True]

p1=Graphics[{PointSize[Large],Black,Point[{1,2.4}],
Text["P",{1,1.5},BaseStyle->{Large,Italic}]}];

p2=Graphics[{PointSize[Large],Black,Point[{-1.7,-0.37}],
Text["P*P",{-2,-2.5},BaseStyle->{Large,Italic}]}];

l1=Plot[x+1.4,{x,-5,5},PlotStyle->{Orange,Dashed}];

c2=Show[c1,l1,p1,p2]

l2=Plot[1.3x+2.2,{x,-5,5},PlotStyle->{Orange,Dashed}];

p3=Graphics[{PointSize[Large],Black,Point[{0,2.25}],
Text["Q",{-0.5,3.2},BaseStyle->{Large,Italic}]}];

p4=Graphics[{PointSize[Large],Black,Point[{-1.7,0}],
Text["P",{-2.1,0.8},BaseStyle->{Large,Italic}]}];

p5=Graphics[{PointSize[Large],Black,Point[{3.35,6.5}],
Text["P*Q",{2,7},BaseStyle->{Large,Italic}]}];

c3=Show[c1,l2,p3,p4,p5]


l3=Plot[2(x-1.2)+2.2,{x,-5,5},PlotStyle->{Orange,Dashed}];

p6=Graphics[{PointSize[Large],Black,Point[{-1,-2.1}],
Text["O",{-0.6,-2.9},BaseStyle->{Large,Italic}]}];

p7=Graphics[{PointSize[Large],Black,Point[{1.7,3}],
Text["O*(P*Q)",{3,2},BaseStyle->{Large,Italic}]}];

c5=Show[c3,l3,p6,p7]


l4=Graphics[{Orange,Dashed,Line[{{3.35,-10},{3.35,10}}]}];
```

```
p8=Graphics[{PointSize[Large],Black,Point[{3.35,-6.6}],
Text["P+Q",{2,-7},BaseStyle->{Large,Italic}]}];

c6=Show[c3,l4,p8]


cir=Graphics[Circle[{1,3.2},4.1]];

p9=Graphics[{PointSize[Large],Black,Point[{0.9,3.3}],
Text["R",{1,4},BaseStyle->{Large,Italic}]}];

c7=Show[c3,cir,p9]
```

References

[1] Silverman, J. H., & Tate, J. T. (2015). Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics) (2nd ed. 2015 ed.). Springer.