Elliptic Curve Triangle Parametrization

L. Maloney A. Tao R.S. Williams

December 19, 2011

Abstract

Let F be a family of triangles with fixed area, A, and perimeter, P. We show that F is parametrized by an elliptic curve of the form $x^2y + xy^2 = k(xy - 1)$ where $k = \frac{P^2}{4A}$. We then go on to show the correspondence between points on such curves and the triangles they represent. A few basic properties of elliptic curves are then discussed, followed by a computation of the torsion and rank of several of these parameterizing elliptic curves. We then show how two curves with distinct k-values can lead to isomorphic curves by examining the j-invariant. Lastly, we attempt to provide a geometric construction which can be applied to any triangle within a given family.

1 Triangle Parametrization

Suppose we are interested in the family of all triangles which have the same area and same perimeter. We may ask ourself the following question:

Is there a way to parametrize families of triangles which have the same area and perimeter?

We claim that elliptic curves of the form $x^2y + xy^2 = k(xy - 1)$ indeed parametrize such families.

Suppose we have a family of triangles with fixed perimeter, P, and area, A, then the radius of the incircle of these triangles is given by $r = \frac{2A}{P}$.

Now we consider the following triangle:

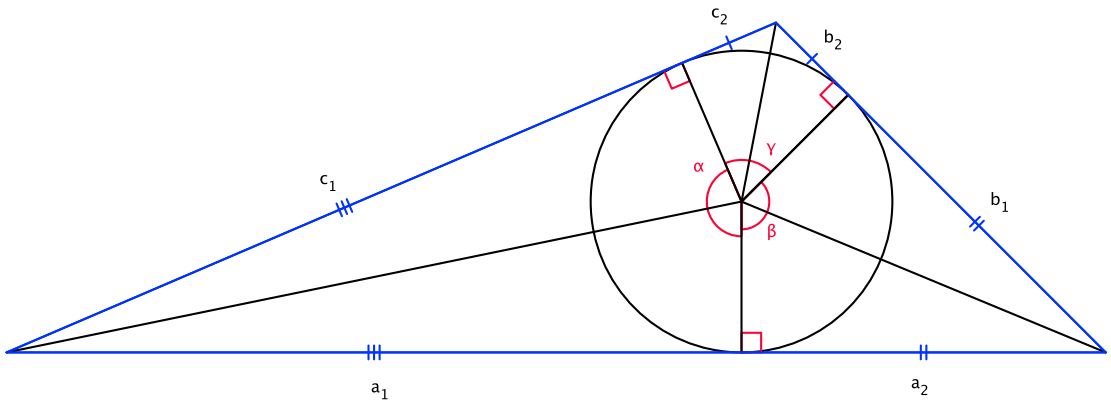


Figure 1: Triangle with Incircle

with

$$a = a_1 + a_2,$$
$$b = b_1 + b_2,$$
$$c = c_1 + c_2.$$

Recall the semiperimeter of a triangle is given by $s = \frac{1}{2}P = \frac{1}{2}(a+b+c)$, however, we could also define s in terms of our angles α, β, γ. Notice that

$$\begin{aligned} s &= \frac{a+b+c}{2} \\ &= \frac{(a_1+a_2)+(b_1+b_2)+(c_1+c_2)}{2} \\ &= \frac{2a_1+2b_1+2c_1}{2} \\ &= a_1+b_1+c_1 \\ &= r\left(\frac{a_1}{r}+\frac{b_1}{r}+\frac{c_1}{r}\right) \\ &= r\left(\tan\frac{\alpha}{2}+\tan\frac{\beta}{2}+\tan\frac{\gamma}{2}\right). \end{aligned}$$

Now, let

$$x = \tan\frac{\alpha}{2}, \qquad y = \tan\frac{\beta}{2}, \qquad z = \tan\frac{\gamma}{2},$$

and notice

$$\frac{\gamma}{2} = \pi - \frac{\alpha}{2} - \frac{\beta}{2},$$

so we see

$$\begin{aligned} z &= \tan\frac{\gamma}{2} \\ &= \tan\left(\pi - \frac{\alpha}{2} - \frac{\beta}{2}\right) \\ &= \tan\left(-\frac{\alpha}{2} - \frac{\beta}{2}\right) \\ &= -\tan\left(\frac{\alpha}{2} + \frac{\beta}{2}\right) \\ &= -\left(\frac{\tan\frac{\alpha}{2}+\tan\frac{\beta}{2}}{1-\tan\frac{\alpha}{2}\tan\frac{\beta}{2}}\right) \\ &= \frac{x+y}{xy-1}. \end{aligned}$$

Therefore, since $s = r(x+y+z)$ with both s and r fixed, it follows that families of triangles with a fixed perimeter and area are parametrized by the cubic curve

$$k = x+y+z = x+y+\frac{x+y}{xy-1},$$

or equivalently,

$$x^2y + xy^2 = k(xy-1).$$

1.1 Converting Curve Points to Triangles

Using the above construction we may now state the explicit relation between points on our cubic curve, $C := x^2y + xy^2 = k(xy-1)$, to the side lengths of a triangle. Recall that we have

$$a = a_1 + a_2, \qquad b = b_1 + b_2 \qquad c = c_1 + c_2,$$

and

$$\begin{aligned} x &= \tan\frac{\alpha}{2} = \frac{a_1}{r} = \frac{c_2}{r}, \\ y &= \tan\frac{\beta}{2} = \frac{a_2}{r} = \frac{b_1}{r}, \\ z &= \frac{x+y}{xy-1} = \tan\frac{\gamma}{2} = \frac{b_2}{r} = \frac{c_1}{r}. \end{aligned}$$

So we may write,

$$\begin{aligned} a &= r\left(\frac{a_1}{r}+\frac{a_2}{r}\right) = r(x+y), \\ b &= r\left(\frac{b_1}{r}+\frac{b_2}{r}\right) = r(y+z) = r\left(y+\frac{x+y}{xy-1}\right) = r\left(\frac{x(y^2+1)}{xy-1}\right), \\ c &= r\left(\frac{c_1}{r}+\frac{c_2}{r}\right) = r(x+z) = r\left(x+\frac{x+y}{xy-1}\right) = r\left(\frac{y(x^2+1)}{xy-1}\right). \end{aligned}$$

Thus, given a point (x, y) on our curve C we can obtain the lengths of the sides of our triangle:

$$a = r(x+y), \qquad b = r\left(\frac{x(y^2+1)}{xy-1}\right), \qquad c = r\left(\frac{y(x^2+1)}{xy-1}\right).$$

In practice inverting this procedure is quite simple, i.e. given the lengths of a triangle it is fairly simple to determine the point on our cubic curve C to which it corresponds. While this inverse can be explicitly stated, its computation is quite involved and unnecessary since the computation is much easier given specific values for a, b and c.

Using the interactive geometry, algebra and calculus applications: Cinderella and GeoGebra, several animations were created which show the relationship between the points on our parameterizing elliptic curves and side lengths of the triangles in a given family. These animations can be found here:

- `http://math.arizona.edu/~rwilliams/Cinderella_Parametrization.html`
- `http://math.arizona.edu/~rwilliams/GeoGebra_Parametrization.html`
- `http://math.arizona.edu/~rwilliams/GeoGebra_Parametrization_Small_k.html`

2 Elliptic Curves

We now briefly turn our attention to elliptic curves in general; discussing the group law on rational points, points of finite order, and the torsion and rank of an elliptic curve.

2.1 Rational Points & Lines

A point in the affine plane, $(x_1, \ldots, x_n) \in \mathbb{A}^n$, is a **rational point** if each of the coordinates is rational. Similarly, we say $ax + by + c = 0$ is a **rational line** if a, b, c are rational, and

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

is a **rational cubic** if all of its coefficients are rational.

It is obvious that the line passing through two rational points will be a rational line, and that the intersection of two rational lines will be a rational point. In general, it is not true that the intersection of a rational conic (quadratic curve) with a rational line are rational points. It can be shown that the two points of intersection will be rational if and only if the roots of equation for the intersection (which will be a quadratic) are rational. If we know one of the roots is rational, then since the sum of the roots equals the coefficient of x, which is rational, it follows the second root must also be rational.

This same principle does not work quite so well when we turn our attention to the intersection of a rational line and a rational cubic. The equation for the intersection will now be a cubic, and if we know only one of the roots is rational, then the other two may be both rational or both irrational. However, if we know that two of the points are rational, then it follows the third point must also be rational. For instance, if P and Q are both rational, and we know our line is rational, then the point $P * Q$ is also rational.

If we do only know one rational point on our cubic curve, then we generally can determine another rational point. For instance, we may take the tangent line to the point P on the curve to obtain our new

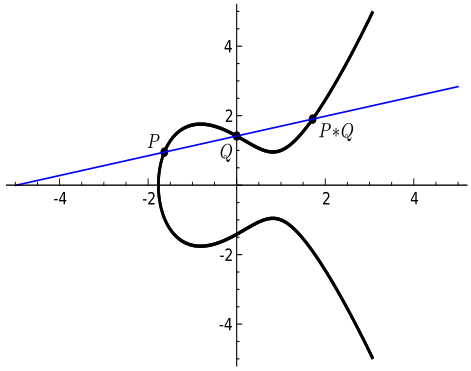


Figure 2: Two Rational Points

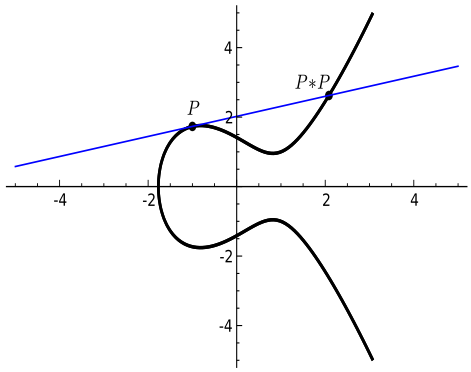


Figure 3: One Rational Point

rational point $P * P$.

Now, we see that given any two points we can find another using our $*$ operation. One can now ask if this $*$ operation defines a group structure on the set of points we generate; however, the answer to this question is no. It is not too difficult to convince oneself that $*$ is associative; however it becomes evident that there is no identity element for our $*$ operation. So, we look to our next section to solve this problem and define a group structure.

2.2 Group Law

Above we saw that a group structure is starting to take shape on a set of points on our cubic, it was only lacking an identity element. We now remedy this problem in the following way:

> Let $\mathcal{O}$ be a fixed point on a cubic curve, C. If P and Q are on C, then to add P and Q, draw the line joining $P * Q$ and $\mathcal{O}$ and define $P + Q$ to be the point where this line intersects C.

Graphically, this is represented as:

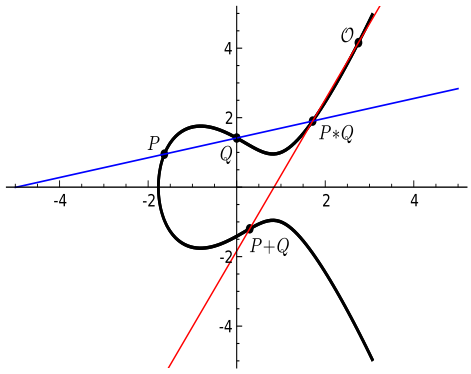


Figure 4: $P + Q$

Again, if we only have one point then we can still calculate $P + P$:

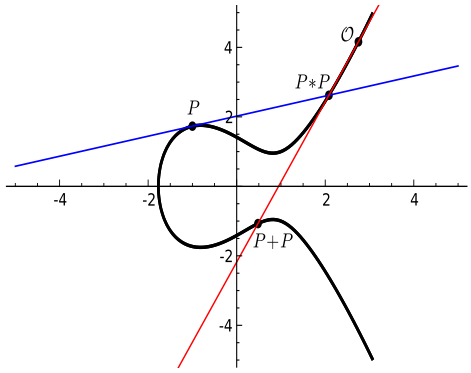


Figure 5: $P + P$

Note that our point $\mathcal{O}$ is the identity element for our addition operation.

Our new group operation leads us to the following theorem:

Theorem 1 (Mordell)**.** *If a non-singular plane cubic curve has a rational point, then the group of rational points is finitely generated.*

Mordell's theorem says that we can get all of the rational points on our curve by starting with a finite set, adding those points to get new points, then adding the new points to get more points, and so on.

2.3 Weierstrass Normal Form

We want to find explicit formulas for our addition operation; however, working with the general equation of a cubic curve,

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

can be quite a task. To make things as simple as possible, it is important to know that any cubic curve with a rational point can be transformed into a special form called **Weierstrass normal form**, of the type

$$y^2 = 4x^3 - g_2x - g_3$$

or the slightly more general form,

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

To transform a general cubic into Weierstrass normal form, first homogenize the curve, $f(X,Y,Z) = C$, so that $C \in \mathbb{P}^2$ is the set of points $[X,Y,Z]$ such that $f(X,Y,Z) = 0$. Now, assume that there is some rational point $\mathcal{O}$ on C, and denote the partial derivatives of f by f_X, f_Y and f_Z. Then the tangent line to $\mathcal{O}$ is given by

$$f_X(\mathcal{O})X + f_Y(\mathcal{O})Y + f_Z(\mathcal{O})Z.$$

Now, define the Z-axis, $Z = 0$ to be this tangent line, meaning

$$Z = f_X(\mathcal{O})X + f_Y(\mathcal{O})Y + f_Z(\mathcal{O})Z.$$

If $\mathcal{O}$ is an inflection point, then we may choose our X-axis to be any line not containing $\mathcal{O}$, say

$$\mathcal{O} \notin X = AX + BY + CZ.$$

If $\mathcal{O}$ is not an inflection point, then our tangent line intersects C at some other point $Q \neq \mathcal{O}$, so take

$$X = f_X(Q)X + f_Y(Q)Y + f_Z(Q)Z.$$

Finally, let

$$Y = aX + bY + cZ,$$

where $\mathcal{O}$ is on the line $L = aX + bY + cZ = 0$, but L is not the tangent line to $\mathcal{O}$ of f.

Defining X, Y and Z in this way gives us a change of coordinate matrix

$$T = \begin{pmatrix} f_X(Q) & f_Y(Q) & f_Z(Q) \\ a & b & c \\ f_X(\mathcal{O}) & f_Y(\mathcal{O}) & f_Z(\mathcal{O}) \end{pmatrix},$$

which is invertible since by our choices the rows are linearly independent. Hence, we may compute X, Y, Z explicitly in terms of x, y, z by calculating

$$T^{-1} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Once we have our equation in the new coordinates X, Y, Z we dehomogenize.

After this we obtain our 'new' equation for C, which will be of the form

$$xy^2 + (ax + b)y = cx^2 + dx + e.$$

Now, multiplying through by x,

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex.$$

Renaming xy to y we obtain

$$y^2 + (ax + b)y = \text{cubic in } x.$$

The cubic in x might not be monic, but another simple substitution can remedy this. Thus, without loss of generality, we may assume C is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Completing the square on the left we have

$$\left(y + \frac{a_1x + a_3}{2}\right)^2 - \left(\frac{a_1x + a_3}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6,$$

where after simplifying we obtain

$$(2y + a_1x + a_3)^2 = 4x^3 + (4a_2 + a_1^2)x^2 + (4a_4 + 2a_1a_3)x + (4a_6 + a_3^2).$$

Making the substitution $y = \frac{1}{2}(y - a_1x - a_3)$ and letting

$$\begin{aligned} b_2 &= 4a_2 + a_1^2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= 4a_6 + a_3^2, \end{aligned}$$

we have

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

which is our 'more general' Weierstrass normal form.

To obtain the other Weierstrass normal form, we begin my making the following substitutions,

$$x = \frac{x - 3b_2}{36} \quad \text{and} \quad y = \frac{y}{108},$$

which give

$$\left(\frac{y}{108}\right)^2 = 4\left(\frac{x - 3b_2}{36}\right)^3 + b_2\left(\frac{x - 3b_2}{36}\right)^2 + 2b_4\left(\frac{x - 3b_2}{36}\right) + b_6.$$

Simplifying, this yields

$$y^2 = x^3 + 27(24b_4 - b_2^2)x + 54(b_2^3 - 36b_2b_4 + 216b_6).$$

If we now let

$$\begin{aligned} c_4 &= 24b_4 - b_2^2, \\ c_6 &= b_2^3 - 36b_2b_4 + 216b_6, \end{aligned}$$

then our equation becomes

$$y^2 = x^3 + 27c_4x + 54c_6,$$

which is our other Weierstrass normal form.

If we trace back through our transformations, we find that

$$(x, y) \longmapsto \left(\frac{x - 12a_2 - 3a_1^2}{36}, \frac{y}{216} - \frac{a_1x}{72} + \frac{a_1a_2}{6} + \frac{a_1^3}{24} - \frac{a_3}{2}\right).$$

2.3.1 Example

If we now consider the elliptic curve $x^2y + xy^2 = 6(xy - 1)$, we can make a substitution $(x, y) \mapsto (-y/x, x^2/y)$ to obtain the 'general' Weierstrass equation

$$y^2 + 6xy + 6y = x^3.$$

In this case we have

$$\begin{aligned} a_1 = a_3 = 6 \\ a_2 = a_4 = a_6 = 0, \end{aligned}$$

so using the transformation defined above, and using one further transformation $(x, y) \mapsto (36x, 216y)$, we have:

$$(x, y) \longmapsto (x - 3, y - 3x + 6).$$

Substituting this into our Weierstrass equation we have

$$(y - 3x + 6)^2 + 6(x - 3)(y - 3x + 6) + 6(y - 3x + 6) = (x - 3)^2,$$

and simplifying we obtain

$$y = x^3 - 9x + 9.$$

If we instead consider an elliptic curve of the form $x^2y + xy^2 = k(xy - 1)$, which we will show in Section 7 to be the cubic curve which parametrizes triangles with fixed perimeter and area, then if $6|k$, it follows that, using the above construction, we will obtain a Weierstrass form with integer coefficients. We can see this if we try to use our substitution

$$(x, y) \longmapsto \left(x - \left(\frac{k^2}{12}\right), y - \frac{kx}{2} + \frac{k^3}{24} - \frac{k}{2}\right),$$

then our equation becomes

$$\left(y - \frac{kx}{2} + \frac{k^3}{24} - \frac{k}{2}\right)^2 + k\left(x - \frac{k^2}{12}\right)\left(y - \frac{kx}{2} + \frac{k^3}{24} - \frac{k}{2}\right) + k\left(y - \frac{kx}{2} + \frac{k^3}{24} - \frac{k}{2}\right) = \left(x - \frac{k^2}{12}\right)^3.$$

Simplifying, we obtain

$$y^2 + \left(\frac{k^4}{48} - \frac{k^2}{2}\right)x + \left(\frac{-k^6}{864} + \frac{k^4}{24} - \frac{k^2}{4}\right) = x^3.$$

To obtain integer coefficients we examine the necessary divisibilities of k and its powers to find that we need $6|k$.

2.4 Group Law Revisited

Above we defined an operation on a set of points on a cubic curve, but our descriptions were mostly geometric, so we now provide explicit algebraic formulas for our addition operation.

Suppose we are given an equation in Weierstrass form,

$$y^2 = x^3 + ax^2 + bx + c,$$

and we homogenize by setting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ to obtain,

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

The line at infinity is given by $Z = 0$, so to find the intersection of this line with our cubic, we substitute $Z = 0$ into the above equation to find $X^3 = 0$, which has a triple root $X = 0$. This means that the cubic meets the line at infinity at $X = 0$ three times, implying that the cubic has only one point at infinity, namely, the point at infinity where vertical lines (i.e. $x =$ constant) meet, and we shall label this point $\mathcal{O}$.

The point $\mathcal{O}$ is counted as a rational point, and as noted above, it represents the identity element under our group addition. Thus, the graphic representation of our addition can now be thought of as follows:

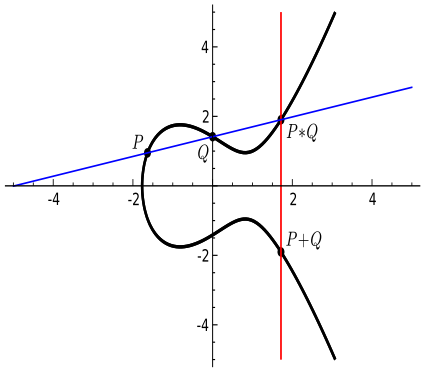


Figure 6: $P + P$

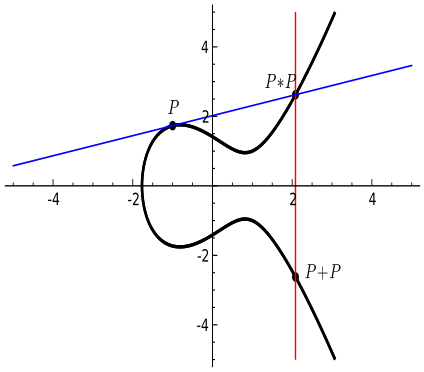


Figure 7: $P + P$

Using this convention, we can now derive explicit formulas for our addition. Suppose we have the following,

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad P_1 * P_2 = (x_3, y_3), \quad P_1 + P_2 = (x_3, -y_3),$$

where P_1 and P_2 are rational points. Then the secant line passing through P_1 and P_2 is given by

$$y = \lambda x + \nu, \qquad \text{where} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Since P_1 and P_2 are rational points, we know that the third intersection point of our secant line with the curve must also be rational. To find this point we substitute and see,

$$(\lambda x + \nu)^2 = y^2 = x^3 + ax^2 + bx + c.$$

Simplifying, we see

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

Now, we know the three roots of this equation are given by x_1, x_2, x_3, so we have

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

Equating the coefficients of our x^2 terms it follows that $\lambda^2 - a = x_1 + x_2 + x_3$, and hence

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + \nu.$$

Note the above derivation only applies if P_1 and P_2 are distinct. If we instead want to compute $P_1 + P_1$, then instead of λ being the slope of our secant line, it will now represent the slope of our tangent line. Hence, if $y^2 = f(x)$ then by implicit differentiation we have

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}.$$

If we now go through our calculations again using this λ, we obtain the **duplication formula**,

$$x \text{ coordinate of } 2(x, y) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

3 Properties of Elliptic Curves and the Group of Heron Triangles

In the following section, we examine some properties of elliptic curves and the group the induce over rational points. Namely, for a curve given by

$$C_k : y^2 + kxy + ky = x^3$$

we identify points of finite order, torsion points, as well as compute the rank of these cures for various values k and, interestingly, identify some values k which give curves of rank 3.

3.1 Background

In this section we introduce the necessary tools in order to develop the study of elliptic curves. As we will see later, elliptic cruves live in projective space and projective geometry, in some sense, is a type of "completion" to our usual affine space.

3.1.1 Projective Geometry

The affine n-space over a field K is the set of n-tuples

$$\mathbb{A}^n(K) = \{(a_1, \ldots, a_n \mid a_i \in K)\}$$

If k is a subfield of K, we make make a completely analogous definition for the k-rational affine space

$$\mathbb{A}^n(k) = \{a_1, \ldots, a_n \mid a_i \in k\}$$

If we take $K = \bar{k}$, i.e. the algebraic closure of k, then we may consider the Galois action on points of the affine n-space where the action is defined coordinate-wise.
For example, if $K = \bar{\mathbb{Q}}$ and $k = \mathbb{Q}$, then we may characterise the $\mathbb{Q}$-rational points in $\mathbb{A}(\bar{A})^n$ by

$$\mathbb{A}^n(\mathbb{Q}) = \{P \in \mathbb{A}^n(\bar{\mathbb{Q}}) \mid \sigma(P) = P \text{ for all } \sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}\}$$

where $G_{\bar{\mathbb{Q}}/\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The projective n-space over K is the $n+1$-tuples

$$\mathbb{P}^n(K) = \{[a_0, \ldots, a_n] \mid a_i \in K \text{ not all zero}\}/\sim$$

where $[a_0, \ldots, a_n] \sim [\alpha a_0, \ldots, \alpha a_n]$ for all $\alpha \in K$.
The coordinates of $\mathbb{P}^n$ are called homogeneous coordinates and which turns out to the natural space to solve homogeneous equations.

Example 2. *Consider integral solutions of the homogeneous polynomial $X^n + Y^n - Z^n = 0$. If (a, b, c) is a solution then $(\alpha a, \alpha b, \alpha c)$ is certainly a solution but since this can be 'generated' by (a, b, c), it makes sense to think of these as the same solutions. Indeed, they are essentially the same point in $\mathbb{P}^n$.*

Remark 1. *$\mathbb{P}^n$ can be covered by $n+1$ $\mathbb{A}^n$'s by*

$$\mathbb{A}^n \hookrightarrow \mathbb{P}^n$$
$$(a_1, \ldots, a_n) \mapsto [a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n]$$

i.e. $\mathbb{P}^n = \mathbb{A}^n_0 \cup \cdots \cup \mathbb{A}^n_n$. Each A^n_i is called an affine chart.

Example 3. *$\mathbb{P}^n(\mathbb{R})$ is covered by $\mathbb{A}^n_i(\mathbb{R})$ and hence is a real manifold if we identify each $\mathbb{A}^n_i$ as Euclidean space. Consider the embedding of $\mathbb{A}^1(\mathbb{R})$ in $\mathbb{A}^2(\mathbb{R})$ by $(a_0) \mapsto (0, a_0)$. Let C be the unit circle centred at $(-1, 0)$, then each point on C not equal $(-1, 1)$, $(-1, -1)$ identifies a unique point on our copy of $\mathbb{A}^1$ via stereographic projection. The the projective line $\mathbb{P}^1$ is then $\mathbb{A}^1 \cup \{\infty\}$, where $\{\infty\}$ is the point at infinity. So $\mathbb{P}^1$ can be identified by the unit circle whereas $\mathbb{A}^1$ is the circle missing two points (note that the circle itself has opposite points identified). It is equivalent then to think of $\mathbb{P}^1$ to be the set of lines going through the origin in A^2. In the literature, $\mathbb{P}^1$ is sometimes called the projective closure or (given an appropriate topology) compactification $\mathbb{A}^1$.*

Remark 2. *In the above example*

$$\begin{aligned}\mathbb{P}^1 &= \{[x, 1]\} \cup \{[1, 0]\} = A^1_0 \cup \{\infty\} \\ &= \{[0, 1]\} \cup \{1, y\} = \{0\} \cup \mathbb{A}^1_0\end{aligned}$$

so by viewing different charts, we may 'move' the point at infinity to the origin and vice versa.

3.1.2 Algebraic Varieties and Rational Functions

An affine algebraic set $V \subseteq \mathbb{A}^n$ is the set of all solutions to a system of polynomial equations in n variables $x_1, \ldots, x_n$. i.e. V is given by

$$V : \begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}$$

A projective algebraic set $V \subseteq \mathbb{P}^n$ is similarly defined to be the set of all solutions to a system of *homogeneous* polynomial equations in $n+1$ variables $x_0, \ldots, x_n$.

A variety is an algebraic set V such that V cannot be expressed as a union of two proper algebraic subsets of V. i.e. $V = U_1 \cup U_2 \implies V = U_1$ or $V = U_2$.

Example 4.

1. *$V = x^2 + y^2 - 1 = 0$ is an algebraic variety over $\mathbb{C}$, we may say $V/\mathbb{C}$ is a variety.*
2. *Let $V : x^2 - 2y^2 = 0$ be an algebraic set over $\mathbb{C}^2$, then $V = U_1 \cup U_2$ where $U_1 : x - \sqrt{2}y = 0$, $U_2 : x + \sqrt{2}y = 0$, so V is not a variety. If the field considered is $\mathbb{Q}$, even though $x^2 - 2y^2$ is irreducible in $\mathbb{Q}[X, Y]$ and is an algebraic variety, V is the empty set over $\mathbb{Q}$.*

A rational function on $\mathbb{A}^n$ is $f \in K(x_1, \ldots, x_n)$.
A rational function on $\mathbb{P}^n$ is either $f = 0$ or $f = \frac{g(x_0,\ldots,x_n)}{h(x_0,\ldots,x_n)}$, where g, h are homogeneous polynomials of the same degree.
The set of rational functions on $\mathbb{P}^n$ and $\mathbb{A}^n$ form a field and are denoted by $K(\mathbb{P}^n)$ and $K(\mathbb{A}^n)$ respectively.

Given an affine variety V/K, we may define the coordinate ring of V to be the set of polynomials over K that do not have any zeroes on V, and is denoted $K[C]$. The field of fractions of the coordinate ring is called function field of V/K. Note that $K(C)$ is a field extension of K, and the transcendence degree of this extension is the dimension of V/K, $\dim(V)$. For a projective variety, we may compute the dimension by taking the intersection of V with an affine chart of the ambient projective space, which is indepedent of choice of chart.

3.1.3 Curves

A projective curve is an infinite algebraic set such that if $X \subseteq C$ is an algebraic set, then X is a finite set. In other words, C is a projective variety of dimension 1.

A projective curve C given by $F(X, Y, Z)$ in $\mathbb{P}$ is singular at P if

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0 = F(P)$$

on some chart of C, otherwise P is non-singular. Note that this definition suggests that non-singular points on C are where the tangent exists on C.

For a curve $C \subseteq \mathbb{P}^n$, let $f = \frac{g}{h} \in K(\mathbb{P}^n)$ be a rational function such that $h \neq 0$ on C. If we restrict f to C, we have

$$f : C \to K$$

and f is called a rational function on C. Such functions form a field, $K(C)$.

Suppose that $C \subseteq \mathbb{P}^m$, $D \subseteq \mathbb{P}^n$. A rational map $\varphi : C \to D$ is a map given by a collection of $f_i \in K(C)$ not all zero as follows:

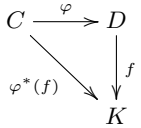
$$\varphi(P) = (f_0(P), \ldots, f_m(P))$$

We say that φ is defined at $P \in C$ if $\exists$ some $g \in K(C)^\times$ such that $f_i g$ is defined at P. If φ is defined for all points on C, we call φ a morphism of C (over K if φ is a rational map over K). If $\exists\ \psi : D \to C$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are identity maps, then φ and ψ are called isomorphisms (over K) and we say that C and D are isomorphic (over K).

A non-constant morphism $\varphi : C \to D$ induces a map on their function fields:

$$\begin{aligned} \varphi^* : K(D) &\to K(C) \\ f &\mapsto \varphi^*(f) := f \circ \varphi \end{aligned}$$

i.e. we have the commutative diagram



Note that φ^* is injective since we have a homomorphism of fields. The degree of φ is the degree of the extension $[K(D) : K(C)]$.

In fact, we have an equivalence of categories between curves and their function fields via the contravariant functor

$$\begin{aligned} C/K &\rightsquigarrow K(C) \\ \{\varphi : C \to D\} &\rightsquigarrow \{\varphi^* : K(D) \to K(C)\} \end{aligned}$$

If $\varphi : C \to D$ is a map of non-singular curves and $\deg(\varphi) = 1$, it can shown easily that φ is a morphism. In particular, we know that C is isomorphic to D since their function fields are isomorphic.

3.1.4 Valuations, Divisors and Differentials

Let $P \in C$ be a non-singular point on a curve, then P defines a discrete valuation on the $K(C)^\times$ by

$$v_P : K(C)^\times \to \mathbb{Z}$$

$$f \mapsto v_P(f) = \begin{cases} n > 0 & f \text{ has zero of order } n \text{ at } P \\ -n < 0 & f \text{ has a pole of order } n \text{ at } P \\ 0 & f(P) \in K^\times \\ \infty & f \equiv 0 \end{cases}$$

This valuation is thought of as "order of vanishing at P" If $v_P(f) = 1$ for some point $P \in C$, then f is called a uniformiser at P.

A divisor D on a curve C is a finite linear combination of points

$$D = \sum_i n_i P_i \qquad n_i \in \mathbb{Z}, P_i \in C$$

i.e. a divisor is a finite formal sum of points on C.

$$\mathrm{Div}(C) = \{\text{divisors of } C\}$$

form an abelian group.
The degree of D is given by

$$\deg(D) = \sum_i n_i \in \mathbb{Z}$$

and the divisors of degree zero, $\mathrm{Div}^0(C)$, form a subgroup of $\mathrm{Div}(C)$.

Any non-constant morphism $\varphi : C \to C'$ with $P = \varphi(Q)$ induces the following homomorphisms on divisors:

$$\begin{aligned} \varphi_* : \mathrm{Div}C &\to \mathrm{Div}C' \\ (Q) &\mapsto (P) \\ \varphi^* : \mathrm{Div}C' &\to \mathrm{Div}C \\ (P) &\mapsto \sum_{\varphi(Q)=P} e_Q(Q) \end{aligned}$$

where φ_* is the pushforward, φ^* is the pull back and

$$e_Q := \text{ ramification index } = v_Q(\varphi^* t_P) \geq 1$$

t_P some uniformiser at P.

Divisors could be defined for functions $f \in K(C)^\times$. The divisor of f is

$$\begin{aligned} \mathrm{div}(f) = (f) : &= \sum_{P \in C} v_P(f) \cdot (P) \\ &= f^*((0)) - f^*((\infty)) \end{aligned}$$

Note that $\deg(f) = 0$ (number of poles = number of zeroes).

$D, D' \in \mathrm{Div}(C)$ that differs by a divisor of a functions are called linearly equivalent (denoted by $\sim$), i.e. $D \sim D'$ if $D - D' = \mathrm{div}(f)$ for some $f \in K(C)^\times$.
$D \sim 0$ are called principal divisors.

Define Picard group as

$$\begin{aligned} \mathrm{Pic}^0(C) &:= \mathrm{Div}^0(C)/\sim \\ \mathrm{Pic}(C) &:= Div(C)/\sim \end{aligned}$$

then it can be shown that $\mathrm{Pic}^0(C)$ is isomorphic to the geometric construction of the group law on elliptic curves by

$$E \simeq \mathrm{Pic}^0$$
$$P \to (P) - (\mathcal{O})$$

for some marked point $\mathcal{O}$ on C.

A differential on a non-singular curve C is a formal finite sum

$$w = \sum_i f_i \, dg_i, \quad f_i, g_i \in k(C)$$

satisfying the following relations

$$\begin{aligned} d(g_1 g_2) &= g_1 dg_2 + g_2 dg_1 \\ d(g_1 + g_2) &= dg_1 + dg_2 \\ da &= 0 \qquad \forall a \in K \end{aligned}$$

For any C, the set of differentials on C forms a 1-dimensional $K(C)-$vector space

$$\{\text{differentials on } C\} = K(C) \cdot df$$

for some $f \in K(C)$.
Furthermore, we can write a differential w as

$$w = f \cdot dt_P, \quad t_P \text{ some uniformiser at } P$$

and with this form, we may associate a divisor with the differential w by

$$\begin{aligned} v_P(w) &:= v_P(f) \\ \operatorname{div}(w) &:= \sum_P v_P(w)(P) \end{aligned}$$

It turns out every differential differs only by a function, so they are all linearly independent. So the set of divisors or differential forms on C span a divisor class $\mathbb{K} \in \operatorname{Pic}(C)$, called the canonical class.

3.2 The Riemann-Roch Theorem and Weierstrass Form

We define a partial order on $\operatorname{Div}(C)$ as follows:
A divisor $D = \sum n_P(P)$ is positive, denoted $D \geq 0$, if $n_P \geq 0$ for every $P \in C$. If $D_1, D_2 \in \operatorname{Div}(C)$, then $D_1 \geq D_2$ means that $D_1 - D_2$ is positive.

For $D \in \operatorname{Div}(C)$, we associate D to the set of functions

$$\mathcal{L}(D) := \{f \in K(C) \mid \operatorname{div}(f) + D \geq 0\}$$

which is a K-vector space with the dimension denoted as $\ell(D)$.

Example 5.

$$\begin{aligned} \mathcal{L} &= \{f \in K(C) \mid div \geq 0\} \quad (\textit{functinos with no poles}) \\ &= K \end{aligned}$$

Example 6. $\mathcal{L}(3(P)) = \{f \in K(C) \mid div(f) \geq -3(P)\}$ *is the set of functions with pole of order at most 3 at P and no other poles anywhere else.*

In general, we can follow the slogan "$\mathcal{L}(D)$ is the functions with a pole at most at D".

Theorem 7 (Riemann-Roch Theorem)**.** *C a non-singular curve. For every $D \in Div(C)$, we have*

$$\ell(D) - \ell(\mathbb{K} - D) = \deg D - g + 1$$

where g is the genus of the curve C, given by

$$g(C) := \ell(\mathbb{K})$$

Elliptic curves are curves of genus 1. If we consider the Riemann-Roch theorem for an elliptic curve E with divisor $D = n(\mathcal{O})$ for some marked point $\mathcal{O}$ on E, we reduce to the following

$$\ell(n(\mathcal{O})) = n \qquad \forall n \geq 1$$

Theorem 8. *Every elliptic curve is isomorphic a curve in Weierstrass form.*

Proof. For a cubic curve E with $\mathcal{O} \in E(K)$:

$$\begin{aligned}
&\mathcal{L}(1(\mathcal{O})) = k =< 1 > \\
&\mathcal{L}(2(\mathcal{O})) =< 1, x > \qquad x \text{ has double pole at } \mathcal{O} \\
&\mathcal{L}(3(\mathcal{O})) =< 1, x, y > \qquad y \text{ has triple pole at } \mathcal{O} \\
&\mathcal{L}(4(\mathcal{O})) =< 1, x, y, x^2 > \\
&\mathcal{L}(5(\mathcal{O})) =< 1, x, y, x^2, xy, > \\
&\mathcal{L}(6(\mathcal{O})) =< 1, x, y, x^2, xy, x^3, y^2 >
\end{aligned}$$

$\ell(6(\mathcal{O})) = 6 \implies$ there is a linear relation between the functions. So

$$\alpha y^2 + \beta x^3 + \cdots = 0$$

and after rescaling $\alpha = 1$ and $\beta = -1$, we obtain

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6$$

□

3.3 Torsion

Theorem 9 ((Nagell-Lutz))**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ with the simplified Weierstrass equation*

$$y^2 = x^3 + ax + b \qquad a, b \in \mathbb{Z}.$$

If $P = (x(P), y(P)) \in E(\mathbb{Q})$ is a non-zero torsion point, then

(i) $x(P), y(P) \in \mathbb{Z}$.

(ii) Either $[2]P = 0$, or $y(P)^2$ divides $4a^3 + 27b^2$.

Remark 3. *The converse statement is not true in general so we may find integral points on the curve satisfying (ii) without being a torsion point.*

Example 10. *Consider our elliptic curve in simplified Weierstrass form given by*

$$E : y^2 = x^3 - 9x + 9$$

then $4a^3 + 27b^2 = 4(-9)^3 + 27(9)^2 = -729 = -3^6$. The possibilities of $y(P)$ are then $0, \pm 3, \pm 9 \pm 27$, where the 2-torsion cases are covered by $y = 0$. We have now reduced the problem to computing integral solutions for the following equations

$$\begin{aligned}
x^3 - 9x + 9 &= 0 \\
x^3 - 9x &= 0 \\
x^3 - 9x - 72 &= 0 \\
x^3 - 9x - 720 &= 0
\end{aligned}$$

We may check for integral solutions by looking for solutions modulo some small primes.

$$\begin{aligned}
x^3 - 9x + 9 = x^3 + x + 1 \ mod\ 2 &\qquad \text{has no solution} \\
x^3 - 9x = x(x^2 - 9) &\qquad \implies x = 0, \pm 3 \\
x/.^3 - 9x - 72 = x^3 - 2x - 2 \ mod\ 7 &\qquad \text{has no solution} \\
x^3 - 9x - 720 = x^3 - 9x + 16 \ mod\ 23 &\qquad \text{has no solution}
\end{aligned}$$

This shows that the only possible *torsion points are $(0, \pm 3), (\pm 3, \pm 3)$.*

By the duplication formula, we compute $[2](0, 3) = (\frac{9}{4}, \frac{3}{8})$ which is not integral, so it is not torsion by Nagell-Lutz, and hence $(0, 3)$ cannot be torsion. Since the inverse of $(0, 3)$ is $(0, -3)$, we know that $(0, -3)$ is not torsion too.

Similarly, we compute that $[2](3, 3) = (3, -3)$ so if we write $P = (3, 3)$, we have $[2]P = -P \implies [3]P = \mathcal{O}$.

To conclude, $E(\mathbb{Q})_{tors} \cong C_3$, the cyclic group of order 3 generated by the point $(3, 3)$.

Theorem 11. *If E had good reduction at p (i.e. $(p, 2\triangle_E)$), then the reduction map:*

$$E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$$

is injective (including the point at infinity).

Example 12. *Let $E : y^2 = x^3 - 9x + 9$ as above with $\triangle_E = -3^6$, so E has good reduction at every prime $p > 3$.*

$$\begin{aligned} p = 5 &\implies \bar{E} : \ y^2 = x^3 + x - 1 \\ &\implies \bar{E}(\mathbb{F}_5) = \{(0, \pm 2), (1, \pm 1), (2, \pm 3), (-2, \pm 2)\} \\ &\implies |\bar{E}(\mathbb{F}_5)| = 9 \end{aligned}$$

$$\begin{aligned} p = 11 &\implies \bar{E} : \ y^2 = x^3 + 2x - 2 \\ &\implies \bar{E}(\mathbb{F}_{11}) = \{(0, \pm 2), (1, \pm 1), (2, \pm 1), (4, \pm 2), (-4, \pm 5), (5, \pm 1), (-5, \pm 2)\} \\ &\implies |\bar{E}(\mathbb{F}_{11})| = 15 \end{aligned}$$

The only group that injects into a group of order 9 and a group of order 15 is C_3.

3.4 Rank

Recall from above that if $C(\mathbb{Q})$ denotes the abelian group of rational points on an elliptic curve, then Mordell's Theorem implies that $C(\mathbb{Q})$ is finitely generated. Hence, by the structure theorem for finitely generated abelian groups,

$$C(\mathbb{Q}) \cong \mathbb{Z}^r \times C(\mathbb{Q})_{\text{tors}},$$

where r is the **rank** of the elliptic curve C.

Unlike the torsion of an elliptic curve, in general there is no known procedure that is guaranteed to compute the rank of an elliptic curve. Programs such as `SAGE` – which uses a combination of `mwrank` (an implementation of 2-descent by Cremona), L-functions, and a database of over 65,000 curves with known rank – does quite well computing ranks, however, there are still curves whose ranks cannot be computed with these programs.

While curves of only relatively small rank have been found, it is conjectured that there exist elliptic curves of arbitrarily large rank. The largest known exactly computed rank of an elliptic curve is 18, which was found by Noam Elkies in 2006. Curves of rank at least 28 are known, however this is only a lower bound, and their exact ranks have not been computed.

3.4.1 Ranks of our Parameterizing Curves

We used SAGE to compute the rank of our parameterizing elliptic curves,

$$x^2y + xy^2 = k(xy - 1)$$

for $k \in \mathbb{Z}$ with $0 \leq k \leq 500$. For the k-values in this range we found $0 \leq r \leq 3$ (or non-computable using SAGE). The computation time varied from a few seconds to upwards of 20 hours for some of the rank 2 curves with k-value above 450. The results of these computations are seen in the following graph: where the k-values with negative rank were the non-computable values. Breaking this down into the

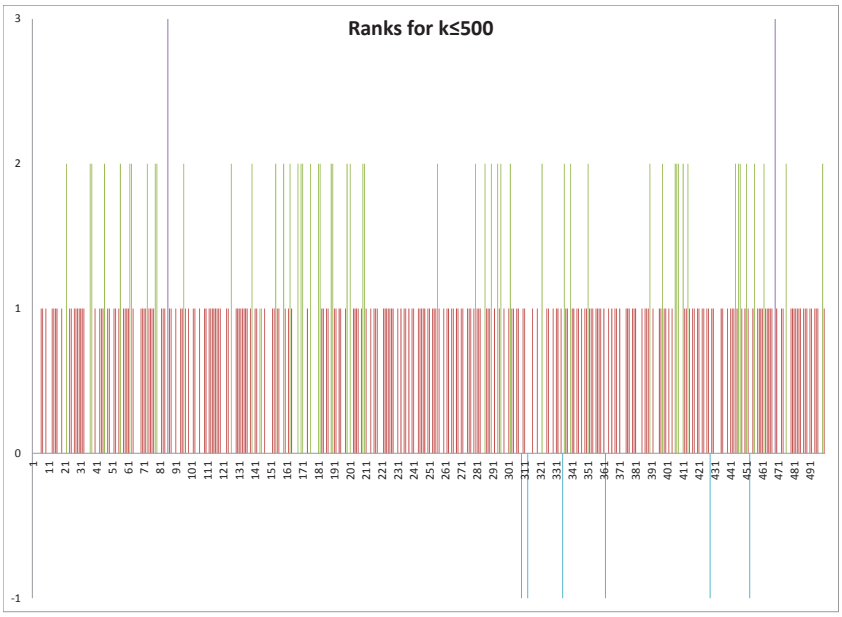


Figure 8: Rank for $0 \leq k \leq 500$

percentages of ranks we have,

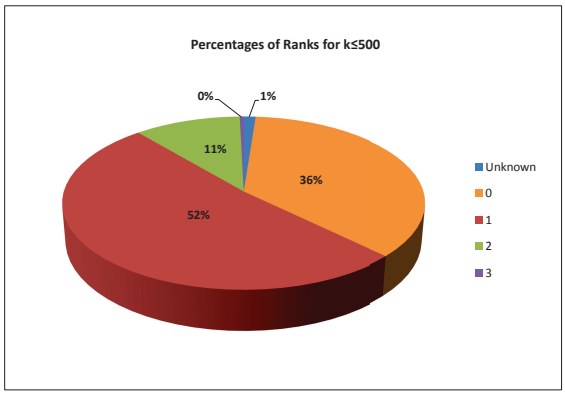


Figure 9: Percentage of Ranks

Note that we only computed the ranks of our elliptic curves for $k \in \mathbb{Z}$, this was simply for a matter of convenience. The ranks could just have easily been computed for any $k \in \mathbb{R}^+$.

4 Isomorphisms of Elliptic Curves

We have seen that we can classify triangle with a fixed area and semi-perimeter via a parameter k. Such a family is given the the elliptic curve in Weierstrass normal from by

$$C_k : y^2 + kxy + ky = x^3.$$

This curve the gives us a group structure that allows us to see that there are infinitely many rational side lengths that give such triangle, those with a fixed rational area and semi-perimeter. Thus arises a natural question: up to isomorphism, do distinct values of k give distinct curves? To examine this question, we introduce a few definitions.

Definition 13. *A rational map*

$$\varphi = [f_0, \ldots, f_n] : V_1 \to V_2$$

is ***regular*** *at $P \in V_1$ if there is some rational function g such that each gf_i is defined for P and there is some i such that $(gf_i)(P) \neq 0$. If a rational map is regular for all P, then it is called a* ***morphism***

Definition 14. *If V_1 and V_2 are varieties, we say that V_1 and V_2 are* ***isomorphic****, if there are morphisms $\varphi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \varphi = Id = \varphi \circ \psi$ where Id is the identity map.*

Remark 4. *Rational is a necessary, but not sufficient condition.*

The language of varieties, seems a bit esoteric for our efforts. However, for our elliptic curves, using properties of smoothness of the curves, we can establish a more concise notion.

Definition 15. *Given a elliptic curves E and $\overline{E}$ defined over a field K, we say that E is* ***isomorphic*** *to $\overline{E}$ if there exists a smooth rational change of coordinates between E and $\overline{E}$.*

We have see that we can put an arbitrary elliptic curve E in the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

called the Weierstrass Normal form. If we wish to know to which extent this form is unique and, in particular, fix the line at infinity, we have the following proposition.

Proposition 16. *If we want to fix the line at infinity, the only change of variables fixing the point chosen and preserving the Weierstrass Normal Form for E is*

$$(x, y) \mapsto (u^2x' + r, u^3y' + u^2sx' + t), \qquad u, r, s, t \in \overline{K}, u \neq 0.$$

We have seen that if $char(K) \neq 2, 3$, we can put our equation into the form

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

called the *Reduced Weierstrass Form.* In this form, we can obtain a refinement for the previous proposition,

Proposition 17. *If we want to fix the line at infinity, the only change of variables fixing the point chosen and preserving the Reduced Weierstrass Form for E is*

$$(x, y) \mapsto (u^2x', u^3y'), \qquad u \in \overline{K}, u \neq 0.$$

Definition 18. *Given an elliptic curve E in Weierstrass Normal form:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define the values,

$$b_2 = (a_1)^2 + 4a_2 \qquad b_4 = 2a_4 + a_1a_3$$

$$b_6 = (a_3)^2 + 4a_6 \qquad b_8 = (a_1)^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2(a_3)^2 - (a_4)^2$$

$$c_4 = (b_2)^2 - 24b_4 \qquad \Delta = -(b_2)^2b_8 - 8(b_4)^3 - 27(b_6)^2 + 9b_2b_4b_6.$$

We call the value Δ the ***discriminant*** *of the curve.*

The values above may seem to the reader to be esoteric, but they simply come from the process of trying to to put the elliptic curve E into Reduced Weierstrass Form via completing the square and the cube, which we may do if $char(K) \neq 2, 3$ where K is the field over which E is defined. i.e. if $char(K) \neq 2$, we can complete the square.

$$\begin{aligned} y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 &\Leftrightarrow y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6 \\ &\Leftrightarrow \left(y + \frac{a_1x + a_3}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1x + a_3}{2}\right)^2 \end{aligned}$$

so, replacing y with $\left(\frac{y - a_1x - a_3}{2}\right)$

$$\begin{aligned} y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 &\Leftrightarrow \frac{y^2}{4} = x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}(a_1^2x^2 + 2a_1a_3x + a_3^2) \\ &\Leftrightarrow y^2 = 4x^3 + (4a_2 + a_1^2)x^2 + 2(2a_4 + a_1a_3)x + (4a_6 + a_3^2) \\ &\Leftrightarrow y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \end{aligned}$$

Thus, the values b come from completing the square and simplifying the expression. Similarly, the c values come from completing the cubic if $char(K) \neq 3$. We now define the notion of the j-invariant of a curve.

Definition 19. *Given an elliptic curve E in Weierstrass Normal form:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

*and the values defined as above, we define the **j-invariant** of the curve E, to be the value,*

$$j = \frac{(c_4)^3}{\Delta}.$$

When two curves are being discussed, we will use the notation j_E for the j-invariant of the curve E.

The values above allow for a useful characterization of elliptic curves. In particular we get the following theorem.

Theorem 20. *Suppose E, $\overline{E}$ are elliptic curves defined over a field K, $charK \neq 2, 3$, given by in Weierstrass Normal form:*

$$E, \overline{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then, E and $\overline{E}$ are isomorphic over $\overline{K}$ (the algebraic closure of K) if and only if

$$j_E = j_{\overline{E}}.$$

Proof. Since $char(K) \neq 2, 3$, we may assume that the curves are given in Reduced Weierstrass form as:

$$E : y^2 = x^3 + Ax + B \qquad \text{and} \qquad \overline{E} : y^2 = x^3 + \overline{A}x + \overline{B}.$$

It is easy to check that, for an elliptic curve C is Reduced Weierstrass form,

$$j_C = \frac{1728(4A)^3}{16[4(A)^3 + 27(B)^2]}.$$

Then, if $E \cong \overline{E}$, then there is some $u \in \overline{K}^*$ such that the isomorphism is given by $(x, y) \mapsto (u^2x, u^3y)$. In particular, we have

$$\frac{A}{u^4} = \overline{A} \qquad \text{and} \qquad \frac{B}{u^6} = \overline{B}.$$

Thus,

$$\begin{aligned} j_{\overline{E}} &= \frac{1728(4\overline{A})^3}{16[4(\overline{A})^3 + 27(\overline{B})^2]} \\ &= \frac{1728\left(4\frac{A}{u^4}\right)^3}{16[4(\frac{A}{u^4})^3 + 27(\frac{B}{u^6})^2]} \\ &= \frac{u^{12}}{u^{12}} \frac{1728(4A)^3}{16[4(A)^3 + 27(B)^2]} \\ &= j_E \end{aligned}$$

For the converse, suppose that $j_E = j_{\overline{E}}$. Then, we have

$$\begin{aligned} \frac{1728(4\overline{A})^3}{16[4(\overline{A})^3 + 27(\overline{B})^2]} &= \frac{1728(4A)^3}{16[4(A)^3 + 27(B)^2]} \qquad \text{so} \\ \overline{A}^3(4A^3 + 27B^2) &= A^3(4\overline{A}^3 + 27\overline{B}^2) \qquad \text{thus} \\ \overline{A}^3 \cdot 4A^3 + \overline{A}^3 \cdot 27B^2 &= A^3 \cdot 4\overline{A}^3 + A^3 \cdot 27\overline{B}^2 \qquad \text{and} \\ \overline{A}^3 \cdot B^2 &= A^3 \cdot \overline{B}^2 \end{aligned}$$

We need only exhibit an isomorphism of the form $(x, y) \mapsto (u^2\overline{x}, u^3\overline{y})$. We consider three cases.

$A = 0$ If $A = 0$ then, since the j-invariant is defined, $B \neq 0$, Then, we must have that $\overline{A} = 0$, and fom the equation above, $u = \left(\frac{B}{\overline{B}}\right)^{1/6}$ gives the desired isomorphism, as

$$y^2 = x^3 + B \longrightarrow \frac{B}{\overline{B}} y^2 = x^3 + B \Leftrightarrow y^2 = x^3 + \overline{B}.$$

$B = 0$ If $B = 0$, then $A \neq 0$. So, from above, we must have that $\overline{B} = 0$. Let $u = \left(\frac{A}{\overline{A}}\right)^{1/4}$. Then,

$$y^2 = x^3 + Ax \longrightarrow \left(\frac{A}{\overline{A}}\right)^{3/2} y^2 = \left(\frac{A}{\overline{A}}\right)^{3/2} x^3 + \left(\frac{A}{\overline{A}}\right)^{1/2} Ax \Leftrightarrow y^2 = x^3 + \overline{A}x$$

$A, B \neq 0$ In this case, taking either $u = \left(\frac{A}{\overline{A}}\right)^{1/4}$ or $u = \left(\frac{B}{\overline{B}}\right)^{1/6}$ will give the desired isomorphism.

□

The reader should take into account the following remarks.

Remark 5. *In Theorem 20 we make the supposition that $char(K) \neq 2, 3$. It should be noted that the theorem still hold for a field K of any characteristic; however, since we are working over $\mathbb{Q}$, we omit the proof for those cases.*

Remark 6. *Additional hypothesis are necessary for the two forms to necessarily preserve the group structure.*

From Theorem 20, we can see that to answer the question of the uniqueness of curves parametrizing our various families of triangles, we need only look at the j-invariants the curves.

Note that we can parametrize the various families of our elliptic curves via the parameter k. We obtain,

$$C_k : y^2 + kxy + ky = x^3.$$

From the definition above, we have the values, $a_1 = k = a_3$, whence we obtain the values,

$$\begin{aligned}
b_2 &= (a_1)^2 + 4a_2 && = k^2 \\
b_4 &= 2a_4 + a_1a_3 && = k^2 \\
b_6 &= (a_3)^2 + 4a_6 && = k^2. \\
b_8 &= (a_1)^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2(a_3)^2 - (a_4)^2 && = 0 \\
c_4 &= (b_2)^2 - 24b_4 && = k^4 - 24k^2 \\
\Delta &= -(b_2)^2b_8 - 8(b_4)^3 - 27(b_6)^2 + 9b_2b_4b_6 && = k^6 - 27k^4 \\
j &= \frac{(c_4)^3}{\Delta} && = \frac{k^6(k^2-24)^3}{k^4(k^2-27)}
\end{aligned}$$

Since k represents the physical quantity of s/r, we are not concerned with $k \leq 0$. Thus, we have that

$$j_{C_k} = j(k) = \frac{k^2(k^2-24)^3}{k^2-27}.$$

Upon inspection, one can see that this function is not one to one. The following figure gives the graph of j as a function of k.

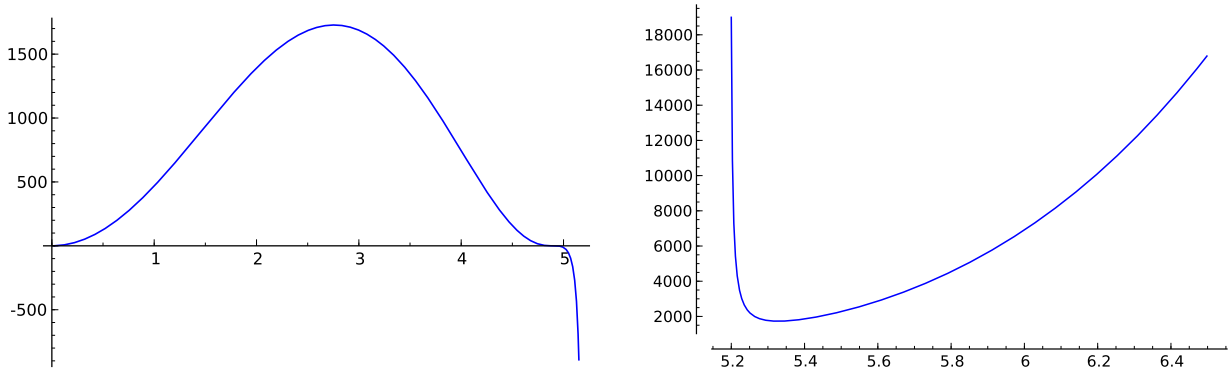


Figure 10: A plot of $j(k)$ with $k \in (0, 5.1)$ and $k \in (5.2, 6.5)$.

From Figure 10, we can clearly see that there stands to be isomorphic copies of curves with a given parameter k. In particular, we examine the family with the $3, 4, 5$ triangle. Recall that this family is given by $k = 6$. We then have $j(6) = 6912$. If we solve the equation, $\frac{k^2(k^2-24)^3}{k^2-27} = 6912$ for k; after disregarding negative and non-real solutions, we find that there is another solution,

$$k = 2\sqrt{3(1+\sqrt[3]{2})}.$$

We let $\alpha = 2\sqrt{3(1+\sqrt[3]{2})}$. It is not difficult, but computationally tedious, to see that the two curves in Reduced Weierstrass form are given by,

$$C_6 : y^2 = x^3 - 9x + 9 \qquad C_\alpha : y^2 = x^3 - 3[1 - \sqrt[3]{4}]x + 3[1 - \sqrt[3]{2}] \tag{1}$$

So, returning to the question of whether or not each family of triangles are unique up to isomorphism, we see that, over some extension of $\mathbb{Q}$, these curves have an isomorphic copy.

4.1 Further Remarks on the j-Invariant

There are a couple of important things that are worth noting in our study of the j-invariant. First, we have that following proposition.

Proposition 21. *For the parameter k as described above, the smallest value k can obtain is $k = 3\sqrt{3}$, which is realized by an equilateral triangle.*

Proof. We can view k as a function of x and y,

$$k(x, y) = \frac{x^2y + y^2x}{xy - 1}.$$

We find that k obtains a local minimum at $x = \sqrt{3} = y$, for which $k(x, y) = 3\sqrt{3}$ which is the only local minima, for positive values of x and y, Further, for a triangle with the property $x = y = \sqrt{3}$, we have $z = \dfrac{x + y}{xy - 1} = \sqrt{3}$, from which it follows easily that the triangle is equilateral. □

From Proposition 21, we can see that only $k \geq 3\sqrt{3}$ represent families of triangles, at least in the typical way we think of triangle in the plane. Also, this allows us to think of the value of k as some sort of measure of how close a triangle is to being equilateral. Moreover, for such values of k, we state the following remark which, similar to the above proposition, can be easily verified using simple calculus.

Remark 7. *For $k \geq 3\sqrt{3}$, $j(k)$ obtains a local minimum at $k = \sqrt{6(3 + \sqrt{3})}$, where $j = 1728$. If we consider all positive k, we also have that $j(k)$ obtains a local maximum at $k = \sqrt{6(3 - \sqrt{3})}$, where $j = 1728$.*

This is an interesting result as it has come to my attention that curves with j-invariant equal to 1728 have some particularly nice properties.

5 Isomorphism of Curves that Parametrize Heron Triangles and Geometric Constructions

The j-invariant of an elliptic curve gives a useful algebraic characterization of the curves we consider; those which parametrize a family of Heron triangles. It gives us a useful, algebraic notion of the isomorphism between any two such curves(defined over some subfield of $\overline{\mathbb{Q}}$). In particular, the proof of Theorem **??**, since $B/B' = \dfrac{9}{3[1 - \sqrt[3]{2}]}$ shows that the map,

$$(x, y) \mapsto (u^2x, u^3y) \qquad \text{where} \quad u = \left(\frac{k_{3,4,5}^2}{k_\alpha^2}\right)^{\frac{1}{6}}.$$

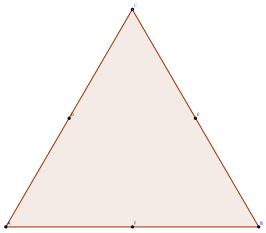
gives an explicit isomorphism between the curves C_6 which represents the family containing the $3, 4, 5$-triangle and C_α which is its isomorphic copy, and does so in an intriguing closed form. However, to truly understand what this isomorphism means in terms of where specific triangles get mapped, requires the computationally cumbersome process of converting a triangle to a point on our general curve, then to Reduced Weierstrass Form, then applying the isomorphism, and returning to the general equation. It would be an elegant and surprising result if we could find a geometric construction which gives a triangle of one family from a construction on a triangle in the family's isomorphic copy. To that end we present the following (continuing work) and ideas.

5.1 Geometric Construction on Heron Triangles

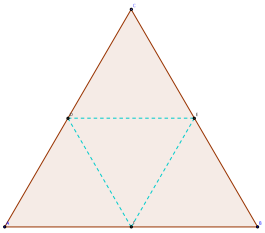
We wish to find a geometric construction that we can apply to any triangle in a family for a particular k-value. In particular, we ask ourselves, is there some object which we can assign to such a triangle. To that end, we offer the following definition.

Definition 22. *To polygon P we associate a polygon P' called the **dual of** P where the vertices of P correspond to edges of P' and vice versa.*

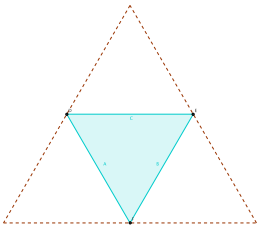
We can assign a dual to every triangle, which is promising. However, as one can see, the definition above is a rather vague one. Actually, there are many different was one could go about assigning a dual. Consider the following example.



Step 1: Bisect the angles, identify their opposite intersection;



Step 2: Draw the triangle obtained by connecting the intersections;



Step 3: Retract the vertices of the old triangle to the sides of the new one.

Example 23. *For a triangle ABC, we can construct the dual of ABC as follows,*

From the construction in Example 23, one can see that for this notion of the dual, the equilateral triangle is dual to itself i.e. when one takes the dual of an equilateral is an equilateral triangle. This is a heuristically promising property since,

$$j(k) = \frac{k^2(k^2-24)^3}{k^2-27}$$

is undefined at $k = 3\sqrt{3}$ which we have seen in Proposition 21 is the k-value for the equilateral triangle. Thus, one would hope that this property of taking the dual of an equilateral triangle, would not produce a triangle in another family.

As we have remarked, there are many different notions for constructing the dual of a polygon. In choosing a method for taking the dual of a triangle, we make the following observations: Recall that the particular k values in question are,

$$k = 6 \qquad \text{and} \qquad k = 2\sqrt{3(1+\sqrt[3]{2})}.$$

- From above, we should have that the equilateral triangle is self dual.
- The number $\sqrt[3]{2}$ is a non-constructible number.
- Classically, angle trisection is not constructible,
- Moreover, we have a triple angle formula given by,

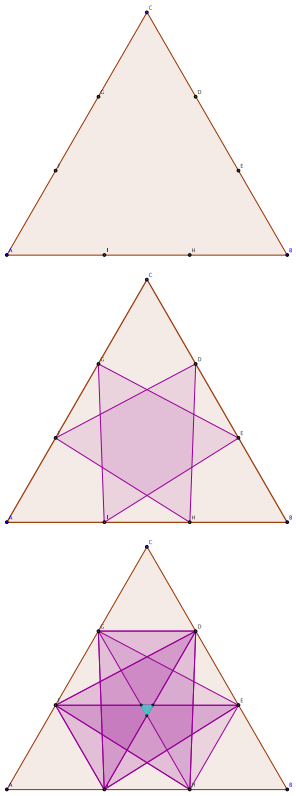
$$\frac{3\tan(\theta)-\tan^3(\theta)}{1-3\tan^2(\theta)}.$$

Angle trisection seems like a reasonable starting point for a construction. We offer the following construction and simultaneously (though not rigorously) show that the construction agrees with the equilateral triangle's being self dual.

Step 1 Trisect each angle, and identify where the trisectors intersect the opposite side.

Step 2 Draw in all the triangles between those points.

Step 3 Identify the triangle where they intersect.



From the picture, it appears that the equilateral remains self-dual under this particular construction. This is promising, so we apply this process to the $3, 4, 5$-triangle (see Figure 11).

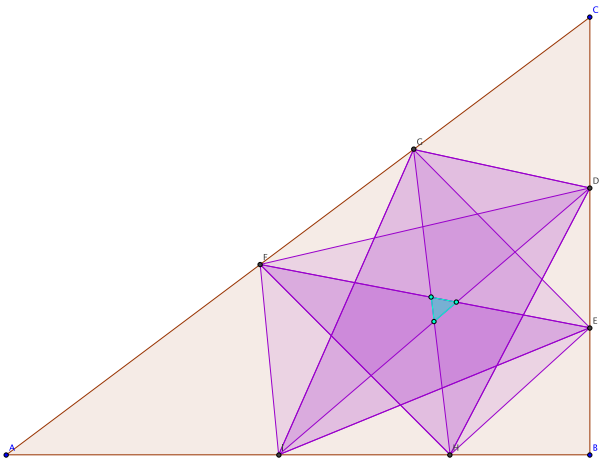


Figure 11: The trisection dual of the $3, 4, 5$-triangle.

Recall that k can be seen as a measure of how much a triangle deviates from being equilateral. The triangle T in figure 11 obtained by the trisection, looks like it is close to being equilateral, however, a quick computation shows that $k_T \approx 5.3515 \neq 2\sqrt{3(1+\sqrt[3]{2})}$.

However, the notion of finding a geometric construction that represents the isomorphism is an appealing one. For possible future work, we introduce the following theorem.

Theorem 24. ***Morely's Trisection Theorem*** *In plane geometry, for any triangle the three points of intersection of adjacent angle trisectors form an equilateral triangle.*

It should be noted that Morely's Trisection Theorem does not hold in spherical or hyperbolic geometry. It would be worth investigating a canonical way to preform this construction on a sphere, as small deviations in k can produce large deviations from being equilateral.

References

[1] Silverma, J.H., Tate, J. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[2] Silverman, J.H. *The Arithmetic of Elliptic Curves. Second Edition.* Graduate Texts in Mathematics. Springer-Verlag, 2009.