ADDITION LAW ON ELLIPTIC CURVES

JORDAN HISEL

Abstract. This paper will explore projective spaces and elliptic curves. Addition on elliptic curves is rather unintuitive, but with a rigorous definition, we will show that the points on elliptic curves themselves are groups under addition. The paper will ultimately prove a lemma central to the proof of associativity of addition on elliptic curves and outline the properties of the operation.

Contents

1. Projective Spaces

Considering the problem of classification of algebraic curves, we use projective spaces instead of affine spaces to make things easier. We can construct projective planes by adding points at infinity to the affine plane. The goal of this paper is to study elliptic curves, those curves that can be transformed into a smooth cubic in the projective plane.

In this paper, we will use the real and complex projective spaces, $\mathbb{RP}^2$ and $\mathbb{CP}^2$.

Definition 1.1. A *projective space* is the space of one-dimensional vector subspaces of a given vector space.

Some properties of a projective plane are as follows:

Proposition 1.2. *A projective plane is a set of lines, a set of points, and a relation between the two (an incidence) such that*

- *given any two distinct points, there exists exactly one line incident between them,*
- *given any two distinct lines, there exists exactly one point incident between them,*

Date: 29 August, 2014.

· *there are four points such that there is no line incident with more than two of them.*

$\mathbb{RP}^2$ is an extension of the real affine plane, and $\mathbb{CP}^2$ is an extension of the complex affine plane.

Definition 1.3. $\mathbb{RP}^2 := \{[a : b : c] | (a, b, c) \in \mathbb{R}^3 \backslash \{(0, 0, 0)\}\} / \sim$, where $[a : b : c] \sim [\lambda a : \lambda b : \lambda c]$, $\lambda \in \mathbb{R}\backslash\{0\}$.

Definition 1.4. $\mathbb{CP}^2 := \{[x : y : z] | (x, y, z) \in \mathbb{C}\backslash\{(0, 0, 0)\}\} / \sim$, where $[x : y : z] \sim [\lambda x : \lambda y : \lambda z]$, $\lambda \in \mathbb{C}\backslash\{0\}$.

There are multiple ways in which $\mathbb{RP}^2$ and $\mathbb{CP}^1$ can be constructed. For example, $\mathbb{RP}^2$ can be constructed with a hemisphere and an infinite line (Figure 1). $\mathbb{CP}^2$ is a 4-dimesional object, so it is difficult to visualize it geometrically. However, we can visualize a common construction of $\mathbb{CP}^1$, the complex projective line, being the Reimann sphere, or the extended complex plane (Figure 2).

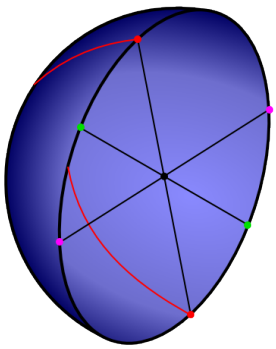


Figure 1 [8]

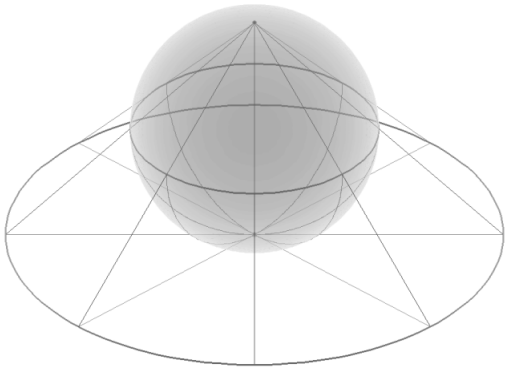


Figure 2 [9]

In order to understand elliptic curves, we must first classify conics in $\mathbb{RP}^2$ and $\mathbb{CP}^2$.

1.1. **Classification of Conics.** The classification of conics in $\mathbb{RP}^2$ and $\mathbb{CP}^2$ is derived from that in $\mathbb{R}^2$ and $\mathbb{C}^2$. We need the following definitions to make such classifications rigorous.

Definition 1.5. An *affine transformation* preserves colinearity and ratios of distances.

Definition 1.6. A set A is *affinely equivalent* to a set B if there exists an affine transformation between the two.

With these terms, we can describe the following lemma:

Lemma 1.7. *Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Any conic in $\mathbb{K}^2$ is affinely equivalent to a prenormal form $y^2 = q(x)$, where $q(x) = Ax^2 + 2Bx + C$ and $A, B, C \in \mathbb{K}$.*

This is a general form of the following lemma, which we will use in our classification of conics in the projective spaces.

Lemma 1.8. *In $\mathbb{R}^2$, any conic is affinely equivalent to one of nine normal forms:*

(1) $y^2 = x$, *parabola;*
(2) $y^2 = -x^2 + 1$, *real ellipse;*
(3) $y^2 = -x^2 - 1$, *imaginary ellipse;*
(4) $y^2 = x^2 + 1$, *hyperbola;*
(5) $y^2 = x^2$, *real line-pair;*
(6) $y^2 = -x^2$, *imaginary line-pair;*
(7) $y^2 = 1$, *real parallel lines;*
(8) $y^2 = -1$, *imaginary parallel lines;*
(9) $y^2 = 0$, *repeated line.*

Proof. By Lemma 1.7, suppose the conic has the form $y^2 = Ax^2 + 2Bx + C$, $A, B, C, \in \mathbb{R}$. If $A \neq 0$, then, under the transformation $x = \lambda x'$,

$$y^2 = Ax^2 + 2Bx + C \xrightarrow{x=\lambda x'} y^2 = A\lambda^2 x'^2 + 2B\lambda x' + C.$$

We can choose λ such that $A\lambda^2 = \pm 1$. For $A > 0$ (resp. $A < 0$), take λ to be $+1$ (resp. -1). Then, completing the square, we get

$$y^2 = \pm x'^2 + 2B\lambda x' + C = \pm(x' - B')^2 + (B'^2 - C') \xrightarrow{(x'-B')=x''} y^2 = \pm x''^2 + D$$

If $D \neq 0$, then let $x'' = \mu\tilde{x}$, $y = \mu y'$. Then we have

$$\mu^2 y'^2 = \pm\mu^2\tilde{x}^2 + D \implies y'^2 = \pm\tilde{x}^2 + \frac{D}{\mu^2}$$

Similar to above, choosing μ such that $\frac{D}{\mu^2} = \pm 1$, we have

$$y^2 = \pm x^2 \pm 1,$$

forms that represent (2) the real ellipse ($y^2 = -x^2 + 1$), (3) the imaginary ellipse ($y^2 = -x^2 - 1$), and (4) the hyperbola, ($y^2 = x^2 + 1$).

Let $B = 0$, $C = 0$, $A \neq 0$. Then, using a similar substitution,

$$y^2 = Ax^2 + Bx^2 + C \implies y^2 = Ax^2 \xrightarrow{y=\alpha y'} \alpha^2 y'^2 = Ax^2 \implies y'^2 = \frac{A}{\alpha^2}x^2$$

We can choose α such that $\frac{A}{\alpha^2} = \pm 1$, so

$$y'^2 = \pm x^2,$$

giving us (5) the real line-pair ($y^2 = x^2$) and (6) the imaginary line-pair ($y^2 = -x^2$).

Consider when $A = 0$ and $B \neq 0$. Then we get (1) the parabola ($y^2 = x$).

$$y^2 = Ax^2 + 2Bx + C = y^2 = 2Bx + C \xrightarrow{2Bx+C=x'} y^2 = x.$$

When $B = 0$, we see

$$y^2 = 2Bx + C \implies y^2 = C.$$

If $C \neq 0$, then, using a similar substitution as above,

$$y^2 = C \xrightarrow{y=vy'} v^2 y^2 = C \implies y^2 = \frac{C}{v^2}$$

Again, we can choose v such that $\frac{C}{v^2} = \pm 1$. This gives

$$y^2 = \pm 1,$$

yielding (7) the real parallel lines ($y^2 = 1$), and (8) the imaginary parallel lines ($y^2 = -1$).

Finally, when $C = 0$, we get (9) the repeated line, $y^2 = 0$. □

A similar lemma is below, which we will not take the time to prove.

Lemma 1.9. *In $\mathbb{C}^2$, any conic is affinely equivalent to one of five normal forms:*

(1) $y^2 = x$, *parabola;*
(2) $y^2 = x^2 + 1$, *general conic;*
(3) $y^2 = x^2$, *line-pair;*
(4) $y^2 = 1$, *parallel lines;*
(5) $y^2 = 0$, *repeated line.*

We can use Lemmas 1.8 and 1.9 to classify conics in $\mathbb{RP}^2$ and $\mathbb{CP}^2$.

Definition 1.10. Two projective curves F, G in $\mathbb{PK}^2$ are *projectively equivalent* if there exists an invertible linear mapping Φ of $\mathbb{K}^3$, and a scalar $\lambda \neq 0$, for which $G = \lambda(F \circ \Phi)$.

Theorem 1.11. *In $\mathbb{RP}^2$, any conic is projectively equivalent to one of five forms:*

(i) $x^2 + y^2 + z^2$, *empty irreducible conic;*
(ii) $x^2 + y^2 - z^2$, *nonempty irreducible conic;*
(iii) $x^2 + y^2$, *imaginary line-pair;*
(iv) $x^2 - y^2$, *real line-pair;*
(v) x^2, *repeated line.*

In $\mathbb{CP}^2$, any conic is projectively equivalent to one of three forms:

(i) $x^2 + y^2 + z^2$, *irreducible conic;*
(ii) $x^2 + y^2$, *line-pair;*
(iii) x^2, *repeated line.*

Proof. We will begin with the real projective conics. Assume the conic has the form $y^2 = Ax^2 + Bxy + Cz^2 + Dzy + Exz$. Since equivalence in the affine plane implies equivalence in the projective plane, we can assume that every real projective conic is equivalent to one of the nine forms in Lemma 1.8.

Assume the given conic has the form $y^2 = \pm xz$, a parabola. Let $xz = z'^2$, and we arrive at (iii;iv) the real and imaginary line pairs.

$$y^2 = \pm z'^2 \implies y^2 - z'^2 = 0.$$

The ellipse $y^2 = -x^2 \pm z^2$ transforms into (i;ii) an empty or nonempty irreducible conic.

$$y^2 = -x^2 \pm z^2 \implies y^2 + x^2 \pm z^2 = 0.$$

The line-pair $y^2 = \pm x^2$ remains (iii;iv) a line-pair, $x^2 \pm y^2 = 0$. Parallel lines ($y^2 = \pm z^2$) are also (iii;iv) line-pairs, shown by letting $z = x$,

$$y^2 = \pm z^2 \implies y^2 \pm x^2 = 0.$$

The repeated line $y^2 = 0$ in affine space remains the repeated line $x^2 = 0$ in projective space.

The arguments for the complex projective plane are similar and will not be covered here. □

2. Ellipic Curves

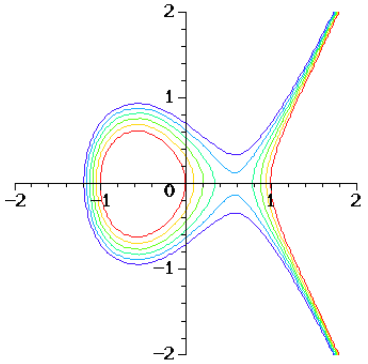
Now we will explore the importance and context of elliptic curves.

Definition 2.1. A curve represented by the homogenous equation $f(X, Y, Z) = 0$ is *smooth* if all derivatives exist and are continuous.

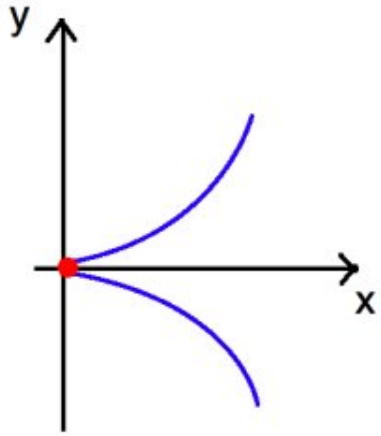
Definition 2.2. An *elliptic curve* is a pair $(E, \mathcal{O})$, a smooth cubic and a specified base point, in the projective plane. It has the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In this paper, we will consider elliptic curves in $\mathbb{CP}^2$.



Elliptic Curves [10]



Not an Elliptic Curve [11]

A common misconception is to mistake elliptic curves for ellipses. The name has its origins for the curves' abilities to help us solve elliptic integrals. These are involved in calculations of the arc length of ellipses and of other shapes such as *Bernoulli's lemniscate:*

$$\int_0^\alpha \frac{dx}{\sqrt{1-x^4}}.$$

3. Addition on Elliptic Curves

In order to define and prove properties of addition of points on elliptic curves, we must first acknowledge the following definition and theorem:

Definition 3.1. The *degree* of an algebraic curve is the degree of the defining polynomial. (A curve is defined by $f(x, y, z) = 0$, polynomial f).

Theorem 3.2 (Bezout's Theorem)**.** *Suppose that X and Y are two plane projective curves defined over a field F that do not have a common component (i.e. X and Y are defined by polynomials whose greatest common divisor is a constant). Then the total number of intersection points of X and Y with coordinates in an algebraically closed field E which contains F, counted with multiplicity, is equal to the product of the degrees of X and Y.*

We will soon see how Bezout's Theorem is central to addition on elliptic curves, as it gives us the following lemma. Addition on elliptic curves would be imposible without Lemma 3.3:

Lemma 3.3. *In a projective plane, let A_{ij} be the intersection points of the straight lines p_i and q_j, where $1 \leq i, j \leq 3$, and the points A_{ij} are pairwise distinct. Suppose*

that all points A_{ij}, except perhaps A_{33}, lie on a cubic. Then A_{33} also lies on this cubic.

Proof. Let $p_i(x,y) = 0$ and $q_j(x,y) = 0$ be the equations of straight lines p_i and q_j, above. Then the third degree equation $p_1p_2p_3 = 0$ determines the triple of lines p_1, p_2, p_3, and the equation $q_1q_2q_3 = 0$ determines the triple of lines q_1, q_2, q_3. By Bezout's Theorem, the cubic $\alpha p_1p_2p_3 + \beta q_1q_2q_3 = 0$ has degree $3 \times 3 = 9$.

Claim: We can represent the equation of any cubic passing through 8 of the 9 points A_{ij} as

$$\alpha p_1p_2p_3 + \beta q_1q_2q_3 = 0.$$

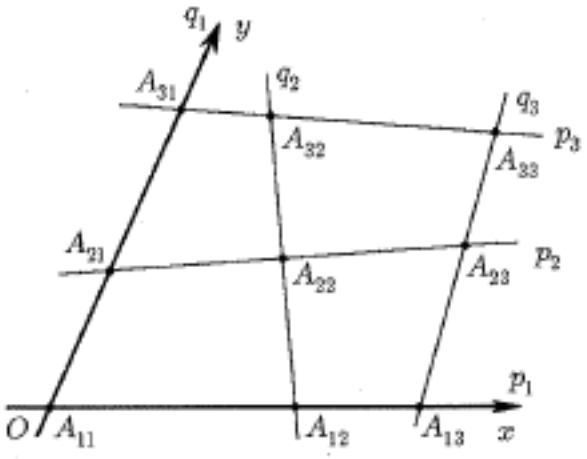


Figure 1 [12]

Proof. Choose a grid such that $p_1(x,y) = y$ and $q_1(x,y) = x$, the coordinate axes. Let the given smooth cubic be called $P(x,y) = 0 \in \mathbb{CP}^2$. The functions $P(0,y)$ and $yp_2(0,y)p_3(0,y)$ vanish at the three points A_{11}, A_{21}, A_{31} on the y-axis. Moreover, these functions are polynomials of degree at most 3. Therefore, $P(0,y) = \alpha y p_2(0,y)p_3(0,y)$ for some $\alpha \in \mathbb{C}$. Similarly, $P(x,y) = \beta x q_2(x,0)q_3(x,0)$ for some $\beta \in \mathbb{C}$. Consider the polynomial

$$Q(x,y) = P(x,y) - \alpha y p_2(x,y)p_3(x,y) - \beta x q_2(x,y)q_3(x,y).$$

It is clear that

$$Q(0,y) = P(0,y) - \alpha y p_2(0,y)p_3(0,y) = 0.$$

Therefore, since $Q(x,y) = a_0(y) + a_1(y)x + a_2(y)x^2 + \cdots$, it vanishes at $x = 0$ iff $a_0(y) = 0$. Therefore, $Q(x,y)$ is divisible by x. Similarly, $Q(x,y)$ is divisible by y. So we have

$$Q(x,y) = xyQ_1(x,y).$$

Since Q is at most a third degree polynomial, Q_1 must be either a linear function or a constant.

Recall that P, p_2p_3, and q_2q_3 all vanish at A_{22}, A_{23}, A_{32}. So Q must also vanish at these points. For each of these points, $xy \neq 0$, so $Q_1(x, y) = 0$ at A_{22}, A_{23}, A_{32}. These points do not lie on a line, so $Q_1(x, y) = 0$, a constant function. Therefore,

$$0 = xyQ_1(x, y) = Q(x, y) = P(x, y) - \alpha p_1p_2p_3 - \beta q_1q_2q_3$$

implies

$$P(x, y) = \alpha p_1(x, y)p_2(x, y)p_3(x, y) - \beta q_1(x, y)q_2(x, y)q_3(x, y)$$

This concludes the proof of the claim. □

Then, $P(x, y) = \alpha p_1p_2p_3 + \beta q_1q_2q_3 = 0$ passes through all points A_{ij}, including A_{33}, concluding the proof of the lemma. □

Remark 3.4. Notice that the proof for Lemma 3.3 only covers cases in which the A_{ij} are pairwise distinct. While the lemma also holds when points coincide, the proof is not covered here.

3.1. **The Operation $\star$.** Now that we've proved Lemma 3.3, we define a binary operation $\star$ on a smooth, irreducible cubic curve $F \subset \mathbb{CP}^2$ as follows:

Definition 3.5. Let $F \subset \mathbb{CP}^2$ be an irreducible curve, and let P, Q be points on F. Suppose that P, Q are distinct with the line $\overline{PQ}$ not tangent at either P or Q. Then, since lines intersect cubics at 3 points, counting multiplicity, there exists a third point R. Then

$$P \star Q := R.$$

But what happens if P, Q are not distinct, or $\overline{PQ}$ is tangent to one of the points?

Definition 3.6. When $\overline{PQ}$ is tangent to F at P,

$$P \star Q = P.$$

Similarly, when $\overline{PQ}$ is tangent to F at Q,

$$P \star Q = Q.$$

Definition 3.7. A point P on F is a *flex*, or *inflection point*, if a change of curvature of F exists at P.

Proposition 3.8. *If $P = Q$, and P is not a flex, then $P \star Q$ is defined to be the point where the tangent line to F at P meets F again. When P is a flex, $P \star Q = P$.*

In order to help us define addition, we check that $\star$ has the following properties.

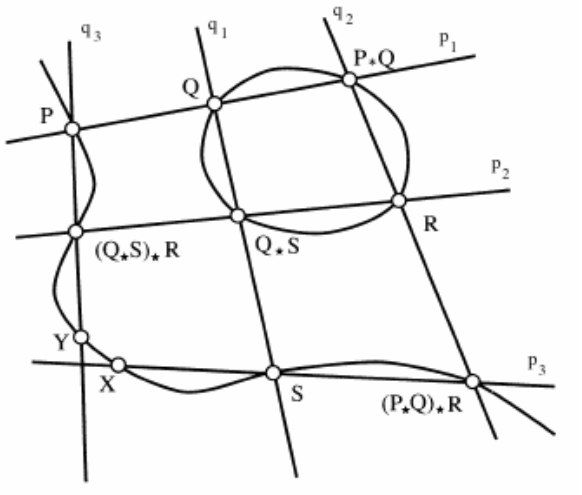
Lemma 3.9. *The binary operation $\star$ has the following basic properties:*

- *(i) (Commutativity) $P \star Q = Q \star P$*
- *(ii) $(P \star Q) \star P = Q$*
- *(iii) $((P \star Q) \star R) \star S = P \star ((Q \star S) \star R)$*

Proof. (i),(ii) follow from the uniqueness of $\overline{PQ}$. (iii) follows from Lemma 3.3. Define the following lines:

$$\begin{array}{lll} p_1 = \overline{PQ} & p_2 = \overline{R, Q \star S} & p_3 = \overline{S, (P \star Q) \star R} \\ q_1 = \overline{QS} & q_2 = \overline{P \star Q, R} & q_3 = \overline{P, (Q \star S) \star R} \end{array}$$

Lemma 3.3 says that if the cubic curves $p_1p_2p_3$ and $q_1q_2q_3$ meet at 9 points, and F, an irreducible cubic curve in $\mathbb{CP}^2$ passes through 8 of them, then F passes through the ninth point.



Let A_{ij} be the intersection points of the above lines, and we know that all A_{ij} lie on F (except perhaps A_{33}), then by Lemma 3.3, A_{33} lies on F. So, by the rules of the $\star$ operation, $A_{33} = ((P \star Q) \star R) \star S$ and $A_{33} = P \star ((Q \star S) \star R)$, giving us

$$A_{33} = ((P \star Q) \star R) \star S = P \star ((Q \star S) \star R).$$

□

4. Addition

We now are able to define addition on elliptic curves.

Definition 4.1. Let $\mathcal{O}$ be the fixed point mentioned above on an irreducible cubic $F \in \mathbb{CP}^2$, P, Q points on F. Define $+$ as $P + Q = (P \star Q) \star \mathcal{O}$.

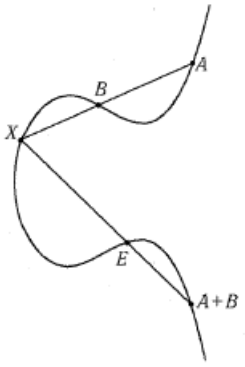


Figure 1 [13]

In Figure 1, E is used to denote $\mathcal{O}$, and maintaining earlier notation, $A = P$ and $B = Q$, and $X = A \star B = P \star Q$. So this shows

$$P + Q = A + B = (A \star B) \star E = X \star E.$$

We will now discuss the properties of $+$.

Lemma 4.2. *The points of F form an abelian group under the operation $+$. The identity element of the group is $\mathcal{O}$. The inverse $-S$ of an element S is given by*

$$-S = S \star (\mathcal{O} \star \mathcal{O}).$$

Proof. We verify that $(F, +)$ satisfies the axioms for groups.

- *Commutativity* Since $\star$ is commutative, then $+$ is commutative.

$$P + Q = (P \star Q) \star \mathcal{O} = (Q \star P) \star \mathcal{O} = Q + P.$$

- *Associativity* We prove associativity using Lemma 3.7(iii).

$$\begin{aligned}(P+Q)+R = ((P+Q)\star R)\star\mathcal{O} &= (((P\star Q)\star\mathcal{O})\star R)\star\mathcal{O}\\ &= (P\star((Q\star R)\star\mathcal{O})\star\mathcal{O}\\ P+(Q+R) = (P\star(Q+R))\star\mathcal{O} &= (P\star((Q\star R)\star\mathcal{O})\star\mathcal{O}\end{aligned}$$

$\mathcal{O}$ is the identity element, again using properties of $\star$:

$$S + \mathcal{O} = (S \star \mathcal{O}) \star \mathcal{O} = (\mathcal{O} \star S) \star \mathcal{O} = S$$

Finally, each element S has an inverse, $-S = S \star (\mathcal{O} \star \mathcal{O})$.

$$\begin{aligned}S + (-S) &= S + (S \star (\mathcal{O} \star \mathcal{O})\\ &= (S \star (S \star (\mathcal{O} \star \mathcal{O}))) \star \mathcal{O}\\ &= ((S \star (\mathcal{O} \star \mathcal{O})) \star S) \star \mathcal{O}\\ &= (\mathcal{O} \star \mathcal{O}) \star \mathcal{O} = \mathcal{O}\end{aligned}$$

□

This proves that the points of elliptic curves compose a group, denoted S_F, under the binary operation $+$.

Acknowledgments. It is a pleasure to thank my mentor, Zhiyuan Ding, for guiding me through the process of understanding elliptic curves, their properties, and their uses.

References

[1] Weisstein, Eric W. "Projective Space." From *MathWorld*–A Wolfram Web Resource. <http://mathworld.wolfram.com/ProjectiveSpace.html>.

[2] Robert Bix. *Conics and Cubics: A Concrete Introduction to Algebraic Curves, Second Ed.* Springer. 1998

[3] C. G. Gibson. *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction.* Cambridge University Press. 1998.

[4] Frances Kirwan. *Complex Algebraic Curves.* Cambridge University Press. 1992.

[5] Viktor Prasolov and Yuri Solovyev. *Elliptic Functions and Elliptic Ingegrals.* American Mathematical Society. 1997.

[6] John H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Ed.* Springer. 1986.

[7] John H. Silverman and John Tate. *Rational Points on Elliptic Curves.* Springer-Verlag. 1992.

[8] Hayate. *Hemisphere Real Projective Plane.* Digital image. Higher Dimensions. phpBB, 21 Mar. 2011. Web. 10 Aug. 2014. <http://hddb.teamikaria.com/forum/viewtopic.php?f=24&t=1605>.

[9] Howison, Mark. *Stereographic Projection in 3D.* Digital image. Complex Projective Space. Wikipedia, 6 Sept. 2007. Web. 10 Aug. 2014. <http://en.wikipedia.org/wiki/Complex_projective_space#mediaviewer/File:Stereographic_projection_in_3D.png>.

[10] Gathen, Joachim von zur, and Jrgen Gerhard. Elliptic Curves. Digital image. Modern Computer Algebra. Bonn-Aachen International Center for Information Technology, 7 May 1999. Web. 10 Aug. 2014.
<https://cosec.bit.uni-bonn.de/science/mca/mca-gallery/mca-elliptic/>.

[11] Cusp. Digital image. Math Problem Solving. Maths Made Easier, n.d. Web. 10 Aug. 2014.
<http://www.math-problem-solving.com/cusp-math-definition.html>.

[12] Viktor Prasolov and Yuri Solovyev. *Affine Grid*. 1997. Image. *Elliptic Functions and Elliptic Integrals*. Page 3. American Mathematical Society. 1997.

[13] Viktor Prasolov and Yuri Solovyev. *Addition on Elliptic Curves*. 1997. Image. *Elliptic Functions and Elliptic Integrals*. Page 2. American Mathematical Society. 1997.

[14] Weisstein, Eric W. "Affine Transformation." From *MathWorld*–A Wolfram Web Resource.
<http://mathworld.wolfram.com/AffineTransformation.html>.

[15] C. G. Gibson. *Properties of the Star Operation*. 1998. Image. *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction.* Page 222. Cambridge University Press. 1998.