



# Equivalence of Real Elliptic Curves

Allen Broughton

Rose-Hulman Institute of Technology

# Credits

---

Discussion with Ken McMurdy

# Outline - 1

---

Why do we care about elliptic curves

What we are trying to prove - main theorem

Real affine elliptic curves - definition and pictures

Projective elliptic curves - definition and pictures

## Outline - 2

---

Group law and intersection with lines

Smoothness, tangents and flexes

Projective linear equivalence

Reduction to Weierstrass normal form

Proof of main theorem

Existence of flexes –via topology

# Why do we care about elliptic curves

---

Probably the most studied object from algebraic geometry and the associated number theory.

The simplest non-trivial algebraic geometric objects

Links to function theory

A group law, and therefore,

Rational elliptic curves have groups that are interesting to cryptographers

## What we are trying to prove

---

An (affine) real elliptic curve is a curve defined by a degree 3 equation with real coefficients

$$f(x,y)=0$$

Two curves are linearly equivalent if one can be mapped on to the other by a linear change of coordinates

## Main theorem

---

- Theorem 1 : A real smooth elliptic curve is (projectively) linearly equivalent to exactly one equation of the form

$$y^2 = x(x-1)(x-\lambda), \quad 0 < \lambda < 1$$

*(two components)*

- or

$$y^2 = x(x^2 - 2\lambda x + 1), \quad -1 < \lambda < 1$$

*(one component)*

# Real affine elliptic curves

## definition and pictures

---

Definition 1. An (affine) real elliptic curve  $E$  is a curve defined by a degree 3 equation with real coefficients. Thus  $f(x,y)$  is a degree three polynomial with real coefficients and

$$E = \{(x,y) \in \mathbf{R}^2 : f(x,y) = 0\}$$

Here are some pictures [pics.mws](#)

# Projective elliptic curves definition and pictures -1

---

An affine real elliptic curve is never compact.

We complete or projectivize a curve by adding points at infinity.

Let  $F(X, Y, Z)$  be a homogeneous polynomial of degree 3 yielding  $f(x, y)$  by dehomogenization i.e.,

$$f(x, y) = F(x, y, 1).$$

For example

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

$$f(x, y) = y^2 - x(x^2 - 1)$$

Two other affine cubics may be obtained by these dehomogenizations:

$$g(x, y) = F(x, 1, z) = z - x(x^2 - z^2) \quad h(y, z) = F(1, y, z) = y^2z - (1 - z^2)$$

## Projective elliptic curves definition and pictures -2

---

Each point  $(x_0, y_0)$  on  $E$  generates a line of zeros of  $F$  since

$$F(ax_0, ay_0, a) = a^3 F(x_0, y_0, 1) = a^3 f(x_0, y_0) = 0$$

Thus the zero set of  $F$  in  $\mathbf{R}^3$  is a cone over  $E$  with the points at infinity satisfying  $Z=0$ . Each line in the cone is called a projective “point” of the curve.

The non-zero triples  $(X:Y:Z)$  are called the homogeneous coordinates of the “point”. The set of all points in the projective plane are denoted  $P(\mathbf{R}^3)$

# Projective elliptic curves definition and pictures -3

---

Here are some pictures [pics.mws](#)

The pictures show the cone, the double cover of the projective curve on the sphere, and the three canonical affine localizations of the projective curve by dehomogenization.

# Group law and intersection with lines -1

---

- Prop 1 A line  $L$  meets a (projective) elliptic curve  $E$  as follows (possibly at infinity)
  - three distinct points - each of contact order 1
  - a tangent and another point contact order 2 and contact order 1
  - a flex or with point contact order 3
- Proof
  - parameterize  $L$  by  $x=at+b$ ,  $y=ct+d$  and the point of intersection are given by  $f(at+b, ct+d)=0$  a cubic in  $t$ .
  - The rest of the proof is this Maple script [lines.mws](#)

## Group law and intersection with lines - 2

---

- Prop 2. Given a point  $P$  on  $E$  there is a birational map  $\varphi : E \rightarrow E$  called projection from  $P$  such that for each  $Q$  on  $E$   $P, Q$  and  $\varphi(Q)$  are collinear
- Prop 3. There is a rational map  $\psi : E \rightarrow E$  such that for each  $Q$  on  $E$  the tangent line at  $Q$  passes through  $\psi(Q)$
- Computational proofs by example [grouplaw.mws](http://grouplaw.mws).
- The group law on the curve is defined in terms of the maps above.

## Smoothness, tangents and flexes -1

---

- Definition 2. An affine curve given by  $f(x,y)=0$  is smooth at  $(x_0,y_0)$  if at least one of the partial derivatives  $\partial f/\partial x$ , or  $\partial f/\partial y$  is non-zero at that point.
- Definition 3. An projective curve is smooth if every point is smooth in each of the three affine local forms.
- Prop 4: a curve is smooth if at least one of  $\partial F/\partial X$ ,  $\partial F/\partial Y$ ,  $\partial F/\partial Z$  is non-zero at every point of the curve.

## Smoothness, tangents and flexes - 2

---

- A smooth curve has a well defined tangent every point.
- A flex is a point with triple contact with the tangent line, the line meets in exactly one point.
- Prop 5: A flex is a fixed point of the tangent line map.
- Prop 6: Real elliptic curves have 3 flexes.

## Projective linear equivalence -1

---

- Definition 4. Two projective elliptic curves  $E_1$   $E_2$  are (projectively) linearly equivalent if there is a linear transformation  $L$  of  $\mathbf{R}^3$  such that  $E_2 = LE_1$  or

$$F_2(X, Y, Z) = F_1(aX + bY + cZ, dX + eY + fZ, gX + hY + iZ)$$

## Projective linear equivalence -2

---

- Prop 7: Given an elliptic curve  $E$  a point  $P$  on the curve, a point  $Q$  in projective space and a tangent direction  $U$  at  $Q$ , then there is a transformation  $L$  mapping  $P$  to  $Q$  and such that  $U$  is the tangent direction of  $L(E)$ .

## Reduction to Weierstrass normal form

---

- An elliptic curve is in Weierstrass normal form if its equation has the form.
$$y^2 = g(x)$$
- for a cubic polynomial  $g(x)$
- Prop 8: If a smooth real elliptic curve has a flex at infinity and is tangent to the line at infinity then it is easily transformed to Weierstrass form.

## Proof of main theorem

---

- Move curve to one which has a flex at the point  $(0:1:0)$  and is tangent to the line at infinity.
- Convert to Weierstrass form  $y^2 = g(x)$
- Convert the polynomial  $g(x)$  to appropriate form.
- [normalform.mws](#)

## Existence of flexes –via topology

---

- By suitable restriction, the tangent line map  $\psi : E \rightarrow E$  defines a map from the circle to the circle.
- Next show that the has degree different from ,1 i.e., that the map is  $d$  to one.
- To prove this it is sufficient to show that from a given point on the circle there is more than one line issuing form the circle that is tangent to the curve this can be done by a topological argument.
- Since the degree is greater than one then there is a fixed point.
- Pictures [tanmap.mws](#)

**All Done**

---

*Any questions?*