Rose-Hulman Institute of Technology

Rose-Hulman Scholar

Mathematical Sciences Technical Reports (MSTR)

Mathematics

8-17-2004

The Birational Isomorphism Types of Smooth Real Elliptic Curves

Sean A. Broughton
Rose-Hulman Institute of Technology, brought@rose-hulman.edu

The Birational Isomorphism Types of Smooth Real Elliptic Curves

S.A. Broughton

Mathematical Sciences Technical Report Series
MSTR 04-05

August 17, 2004

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 **Phone (812)-877-8193**

The Birational Isomorphism Types of Smooth Real Elliptic Curves

S. Allen Broughton
Department of Mathtematics
Rose-Hulman Institute of Technology

August 17, 2004

Contents

1 Introduction

In this note we determine all birational isomorphism types of real elliptic curves and show that it is the same as the orbit space of smooth cubic real curves in $P^2(\mathbb{R})$ under linear projective equivalence. There are two families, each depending polynomially on a real parameter in a open subinterval of $\mathbb{R}$. We further show that the complexification of a real elliptic curve has exactly two real forms. Thus the real elliptic curves come in pairs which are isomorphic over $\mathbb{C}$. Finally, the map taking a real elliptic curve to its j-invariant maps the two families onto the real line in $\mathbb{C}$, intersecting only at the value 1728, the special curve with 4 automorphisms and two topologically distinct real forms.

This paper is self contained and uses nothing more than the basic definitions of algebraic geometry and the computations of, say, college algebra.

2 Definitions and background information

2.1 Real varieties and their complexifications

We assume that the following notions from basic algebraic geometry:

- affine space $A^n(k)$ and projective space $P^n(k)$ over a field k,
- homogeneous coordinates $(X_0 : X_1 : \cdots : X_n)$ of a point in $P^n(k)$,
- definition of an affine and projective variety,
- definition a k-rational map between varieties, and
- definition of a smooth point on a variety.

Definition 1 *For a real projective variety X the complexification, $X_\mathbb{C}$, is the variety over $\mathbb{C}$ obtained by extending scalars to $\mathbb{C}$, i.e., the complex solutions of the defining equations. When needed, we will denote the real points of a variety by $X_\mathbb{R}$.*

Definition 2 *We have four notions of isomorphism for real projective varieties.*

- *Two varieties are birationally isomorphic if there is a bijective, birational map from one variety to the other, defined over $\mathbb{R}$.*
- *Two varieties are ambiently, birationally isomorphic if there is a bijective, birational map, defined over $\mathbb{R}$, between the complexifications of the varieties bijectively carrying real points to real points.*
- *Two varieties are birationally isomorphic over $\mathbb{C}$ if their complexifications are birationally isomorphic over $\mathbb{C}$.*
- *Two real varieties are linearly, projectively isomorphic if there is a linear transformation of $P^n(\mathbb{R})$ carrying one variety bijectively to another. Similarly for varieties defined over $\mathbb{C}$.*

Proposition 3 *If two non-empty real elliptic curves are birationally equivalent then they are ambiently birationally equivalent.*

Proof. Suppose that $E^1_\mathbb{R}$ and $E^2_\mathbb{R}$ are the real parts of two complex curves and $\varphi : E^1_\mathbb{R} \to E^2_\mathbb{R}$ a birational isomorphism. We take this to mean that $E^1_\mathbb{R} \subseteq P^m(\mathbb{R})$ and $E^2_\mathbb{R} \subseteq P^n(\mathbb{R})$ and two rational maps $\varphi^1 : P^m(\mathbb{R}) \to P^n(\mathbb{R})$ and $\varphi^2 : P^n(\mathbb{R}) \to P^m(\mathbb{R})$, such that $\varphi = \varphi^1_{|E^1_\mathbb{R}}$ $\varphi^{-1} = \varphi^2_{|E^2_\mathbb{R}}$. From the definition of complexification and the definitions of rational maps we get extensions $\varphi^1_\mathbb{C} : P^m(\mathbb{C}) \to P^n(\mathbb{C})$ and $\varphi^2_\mathbb{C} : P^n(\mathbb{C}) \to P^m(\mathbb{C})$, $\varphi^1_\mathbb{C}(E^1_\mathbb{C}) \subseteq E^2_\mathbb{C}$ and $\varphi^2_\mathbb{C}(E^2_\mathbb{C}) \subseteq E^1_\mathbb{C}$, whenever these maps are defined. On a smooth curve, every partially defined birational map to projective space extends to a map defined on the entire curve. Thus the maps $\varphi_\mathbb{C} : E^1_\mathbb{C} \to E^2_\mathbb{C}$ and $\varphi^{-1}_\mathbb{C} : E^2_\mathbb{C} \to E^1_\mathbb{C}$ are well defined, and the compositions $\varphi^{-1}_\mathbb{C} \circ \varphi_\mathbb{C}$ and $\varphi_\mathbb{C} \circ \varphi^{-1}_\mathbb{C}$ are the identity on the infinite sets $E^1_\mathbb{R}$ and $E^2_\mathbb{R}$ respectively and hence equal the identity on the complexifications. But we have now produced the maps that explicitly give the ambient birational isomorphism. ■

2.2 Elliptic curves

Definition 4 *A real elliptic curve E is a projective curve whose complexification $E_{\mathbb{C}}$ is a genus 1 curve over $\mathbb{C}$.*

A cubic curve in $P^2(k)$ is a variety given by a single homogeneous equation of degree 3 as in equation 3 in Section 4. It is well known that smooth cubic has a group law but we only need to know that the group of birational automorphisms acts transitively on the points.

Proposition 5 *A smooth cubic in $P^2(k)$ has a transitive group of birational automorphisms, when $k = \mathbb{R}$ or $\mathbb{C}$.*

Proof. We may assume for the purpose of this proof that the curve E is given in the affine plane by a cubic equation of the form $f(x, y) = 0$. First let (x_0, y_0) and (x_1, y_1) be any two distinct points on the curve. We are going show that the line through these two points meets the curve in a third point that is easily computed in terms of the coordinates of the two points. Parameterize the line through the two points and consider f along the line to get a function.

$$k(t) = f(x_0 + t(x_1 - x_0), y_0 + t(y_1 - y_0)).$$

This is a polynomial of degree 3 in t whose coefficients are polynomials in $\{x_0, y_0, x_1, y_1\}$. Since $k(0) = f(x_0, y_0) = 0, k(1) = f(x_1, y_1) = 0$, then $k(t) = t(t-1)(gt - h)$, where $g = g(x_0, y_0, x_1, y_1)$ and $h = h(x_0, y_0, x_1, y_1)$ are polynomials in $\{x_0, y_0, x_1, y_1\}$. The third point occurs when $t = h/g$ and so the point

$$(x_2, y_2) = (x_0 + \frac{g}{h}(x_1 - x_0), y_0 + \frac{g}{h}(y_1 - y_0))$$

is the third point. Now let (x_1, y_1), (x_2, y_2), be any two distinct points on the curve, let (x_0, y_0) be the third point on E meeting the line containing (x_1, y_1) and (x_2, y_2). Define a map $\varphi : E \to E$ by

$$\varphi(x, y) = (x_0 + \frac{g(x_0, y_0, x, y)}{h(x_0, y_0, x, y)}(x - x_0), y_0 + \frac{g(x_0, y_0, x, y)}{h(x_0, y_0, x, y)}(y - y_0)).$$

With a little work on can show that it is a well-defined rational map with an inverse of similar form. By construction, $\varphi(x_1, y_1) = (x_2, y_2)$. It is also clear that if E is defined over $\mathbb{R}$ and (x_1, y_1), $(x_2, y_2) \in E_{\mathbb{R}}$ then φ is a real rational mapping. ■

The following well known fact follows from the Riemann-Roch theorem, and justifies considering only the Weierstrass form in the next section.

Proposition 6 *An elliptic curve is birationally isomorphic to a cubic curve in P^2.*

3 Weierstrass form, double covers, and invariants

Let E be real projective curve. The equation of E is in (non-degenerate) Weierstrass form if it has affine form

$$y^2 = g(x) = a_0x^3 + a_1x^2 + a_2x^1 + a_3$$

with $a_0 \neq 0$. This affine curve may be smoothly completed to obtain E by adding a single real point at infinity which we denote ∞. The real curve $E_{\mathbb{R}}$ and the complexified curve $E_{\mathbb{C}}$ will be both be smooth if and only if $g(x)$ has no multiple roots. Now consider the map $q : E_{\mathbb{R}} \to P^1(\mathbb{R})$ and its complexification $q_{\mathbb{C}} : E_{\mathbb{C}} \to P^1(\mathbb{C})$, given by $(x, y) \to x$. For the real map this is a degree two map with fibres $\{(x, \sqrt{g(x)}), (x, -\sqrt{g(x)})\}$, provided $g(x) > 0$. The fibres are degenerate when $g(x) = 0$ or at $\{\infty\}$ lying over $\infty \in P^2(\mathbb{R})$. A similar statement holds for the complex map except that we replace the condition $g(x) > 0$, with $g(x) \neq 0$. It follows that the real map has two or four branch points and that the complex map always has four branch points. More generally, a double cover is a degree 2 rational map $q : E_{\mathbb{R}} \to P^1(\mathbb{R})$. The map will not be onto though the complexification $q_{\mathbb{C}} : E_{\mathbb{C}} \to P^1(\mathbb{C})$ is surjective with exactly four branch points in $P^1(\mathbb{C})$.

Now let's analyze further a double cover defined by the Weierstrass form. Observe that the image $E_{\mathbb{R}}$ in $P^1(\mathbb{C})$ has either one or two components depending on the number of real roots of $g(x)$. If there are three real roots $\lambda_1, \lambda_2, \lambda_3$ then there are two components which are closed intervals in $P^1(\mathbb{R}) \subset P^1(\mathbb{C})$ whose endpoints are the branch points $\{\lambda_1, \lambda_2, \lambda_3, \infty\}$. If there is one real root λ_1 and two complex roots μ_1, μ_2 then the image is an interval bound by the two real branch points $\{\lambda_1, \infty\}$. Next, consider the closure of the set $\{x : g(x) \leq 0\}$ in $P^1(\mathbb{R})$. The fibres of $q_{\mathbb{C}}$ corresponding to these values of x are of the form. $\{(x, i\sqrt{-g(x)}), (x, -i\sqrt{-g(x)})\}$. These points form a closed subset of $E_{\mathbb{I}} \subset E_{\mathbb{C}}$ which map to the interval(s) complementary in $q(E_{\mathbb{R}})$. The set $E_{\mathbb{I}}$ maps to the real elliptic curve $E^-_{\mathbb{R}}$ defined by $y^2 = -g(x)$ by $(x, y) \to (x, iy)$.

3.1 Cross-ratio and j-invariant

Let w_1, w_2, w_3, w_4 be the four branch points and construct the following cross-ratio

$$\lambda = \frac{(w_4 - w_1)}{(w_4 - w_2)} \frac{(w_3 - w_2)}{(w_3 - w_2)}. \tag{1}$$

The value λ is determined by selecting the unique linear fractional transformation

$$L : z \to \frac{(z - w_1)}{(z - w_2)} \frac{(w_3 - w_2)}{(w_3 - w_2)}$$

satisfying

$$L(w_1) = 0, L(w_2) = 1, L(w_3) = \infty$$

and then defining $\lambda = L(w_4)$. We compute from the cross-ratio the j-invariant defined by

$$j(\lambda) = 256\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Two values λ, λ' give the same j-invariant if and only if

$$\lambda' \in \{\lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{\lambda}{\lambda - 1}, \frac{1}{1 - \lambda}, \frac{\lambda - 1}{\lambda}\}. \tag{2}$$

Indeed, permuting the indices of w_1, w_2, w_3, w_4 in 1 gives the six different values. These transformations form a very famous group of substitutions of the projective line; we shall call it the J-group. The j-invariant is uniquely associated to a branch set and we have the following well-known theorem. A proof may be found in almost any text on elliptic curves. A specific reference is [1].

Proposition 7 *Two complex elliptic curves are birationally isomorphic if and only if their j-invariants are equal.*

In the next section normal Weierstrass forms for real curves are determined. Form the preceding discussion they are of two general types:

- a one parameter family with three real branch points $y^2 = x(x-1)(x-\lambda)$.
- a one parameter family with conjugate complex branch points of unit modulus, $y^2 = x(x-\lambda)(x-\overline{\lambda})$,

The j-invariants are given in Table 1 in the next section.

4 Reduction to a Weierstrass normal form

In this section we find normal forms for real cubic curves under linear projective equivalence. We first note that given any curve X, a point P_0 on X, any other point $Q_0 \in P^2(\mathbb{R})$, and tangent direction $\overrightarrow{u}$ at Q_0, there is a projective linear transformation such that $L(P_0) = Q_0$ and the tangent direction of $L(X)$ is $\overrightarrow{u}$. Moreover the coefficients of the projective linear transformation come from the field generated by the coefficients of P_0, Q_0 and $\overrightarrow{u}$. Recall that a flex is a point on the curve whose tangent line has triple contact with the curve. A projective linear transformation maps a flex of X to a flex of $L(X)$, since it preserves order of contact of curves and takes the tangent line to the tangent line. We will make use of the following, it can be proven in various ways.

Proposition 8 *[?] Every smooth real projective cubic curve has at least one flex.*

Our first task is to put a generic smooth cubic into Weierstrass form. To this end we may assume the following:

- the projective equation of the curve is given by:

$$\begin{aligned} 0 &= F(X,Y,Z) \qquad (3)\\ &= a_0\,X^3 + a_1\,X^2\,Y + a_2\,X\,Y^2 + a_3\,Y^3 \\ &\quad +Z\,(b_0\,X^2 +\, b_1\,X\,Y +\, b_2\,Y^2) + Z^2\,(c_0\,X +\, c_1\,Y) + d_0\,Z^3 \end{aligned}$$

- The point $P_0 = (0:1:0)$ is on the curve and is an inflection point (and, by definition a smooth point).

- The tangent direction of the curve at P_0 is given by $(u,v) = (1,0)$ in the local coordinates $w = X/Y$, $z = Z/Y$ at P_0.

In the local affine coordinates $w = X/Y$, $z = Z/Y$ at P_0 $(w = 0, z = 0)$ the equation of the curve is:

$$0 = h(w,z) = a_0\,w^3{+}a_1w^2{+}a_2\,w{+}a_3{+}z\,(b_0\,w^2{+}\,b_1\,w{+}\,b_2){+}z^2\,(c_0\,w{+}c_1){+}d_0\,z^3 = 0$$

Since P_0 is a smooth point then either

$$a_2 = h_w(0,0) \neq 0, \text{ or } b_2 = h_w(0,0) \neq 0. \qquad (4)$$

Consider an expansion along the tangent direction (u,v) from $(0,0)$

$$\begin{aligned} h(tu,tv) &= h(0,0) + t(uh_w(0,0) + vh_z(0,0)) \\ &\quad + \frac{t^2}{2}(u^2h_{ww}(0,0) + 2uvh_{wz}(0,0) + v^2h_{zz}(0,0)) + t^3K(u,v), \end{aligned}$$

for some degree 3 homogenous polynomial $K(u,v)$. Now $h(0,0) = 0$ so

$$a_3 = h(0,0) = 0 \qquad (5)$$

Along the tangent direction $(u,v) = (1,0)$ the coefficient of t must vanish so $h_w(0,0) = 0$ and

$$a_2 = h_w(0,0) = 0. \qquad (6)$$

Finally, since P_0 is a flex then the coefficient of t^2 must vanish along the tangent direction giving $h_{ww}(0,0) = 0$,giving

$$a_3 = h_{ww}(0,0) = 0. \qquad (7)$$

It follows that

$$F(X,Y,Z) = a_0\,X^3 + Z\,(b_0\,X^2 +\, b_1\,X\,Y +\, b_2\,Y^2) + Z^2\,(c_0\,X +\, c_1\,Y) + d_0\,Z^3$$

In the affine plane, with the affine coordinates $x = X/Z, y = Y/Z$, the equation becomes

$$0 = f(x,y) = a_0\,x^3 + b_0x^2 +\, b_1xy +\, b_2\,y^2 + c_0x +\, c_1y) + d_0$$

or

$$0 = f(x,y) = b_2\, y^2 + (b_1 x + c_1)y + a_0\, x^3 + b_0 x^2 + c_0 x + d_0.$$

Next, make the substitution $y = y - px - q$, solve for p and q to make the y terms vanish, and divide the new $f(x,y)$ by b_2. The values are $p = \frac{b_1}{2b_2}$, $q = \frac{c_1 b_1}{2b_2}$, and we get an equivalent equation.

$$f(x,y) = \, y^2 + \frac{a_0}{b_2}\, x^3 + \frac{\left(-\frac{b_1^2}{4\,b_2} + b_0\right)}{b_2}\, x^2 + \frac{\left(c_0 - \frac{c_1\, b_1}{2\, b_2}\right)}{b_2}\, x - \frac{\frac{c_1^2}{4\, b_2} + d_0}{b_2}$$

We note that dividing by b_2 is legitimate because of the smoothness criterion 4 and the tangency condition 6. Thus by suitable redefinition we may assume that the affine equation is given by

$$y^2 = a_0 x^3 + b_0 x^2 + c_0 x^2 + d_0 = g(x)$$

or

$$f(x,y) = g(x) - y^2 = 0,$$

after suitable redefinition of the coefficients. Also note that the coefficients are real since we always used real coefficients in our transformations. It is well known that the curve is smooth if $g(x)$ has distinct roots, and if there is a singularity then the curve is singular at $(x = \lambda, y = 0)$, where λ is a multiple root of $g(x)$. Furthermore, if there are multiple roots then all roots are real. Now let us find normal forms under the equivalence relation of invertible affine transformations:

$$T(x,y) = (px + qy + r, sx + ty + u)$$

and projective equivalence, i.e. $f \to \frac{1}{w} f \circ T$, for a non-zero real w. Let us apply the transformation. Applying the transformation $f \to f(ax, cy)/c^2$. We get:

$$\frac{a_0 a^3}{c^2} x^3 + \frac{b_0 a^2}{c^2} x^2 + \frac{c_0 a}{c^2} x - y^2.$$

Now we want to find a and c so that $\frac{a_0 a^3}{c^2} = 1$. Then we must have $a_0 a^3 = c^2$, and this can be done by choosing $a = \pm 1$ so that $a_0 a^3 > 0$ and setting $c = \sqrt{a_0 a^3}$. Hence after redefining the coefficients we may assume that $a_0 = 1$. We then have two possibilities, Case I: three distinct real roots

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3), \tag{8}$$

and Case II: one real root, two conjugate complex roots, all distinct,

$$y^2 = (x - \lambda)(x - \mu)(x - \overline{\mu}). \tag{9}$$

Now assume that λ_1 is the smallest root in equation 8. The substitution $(x,y) \to (x + \lambda_1, y)$ yields the equivalent real equation

$$y^2 = x(x - (\lambda_2 - \lambda_1))(x - (\lambda_3 - \lambda_1)).$$

Thus we may assume that the equation is $y^2 = x(x-\lambda_2)(x-\lambda_3)$ with $0 < \lambda_2 < \lambda_3$. Next applying the transformation $(x, y) \to (\lambda_3 x, \sqrt{\lambda_3^3} y)$ we get an equivalent equation

$$y^2 = x(x - \lambda_2/\lambda_3)(x-1) = x(x-\lambda)(x-1) \tag{10}$$

with $0 < \lambda = \lambda_2/\lambda_3 < 1$.

For the complex case II we may use the substitution $(x, y) \to (x + \lambda, y)$ to make the real root zero: $y^2 = x(x-\mu)(x-\overline{\mu})$. Considering the transformation $(x, y) \to (|\mu|\, x, \sqrt{|\mu|^3} y)$ we get $y^2 = x(x - \mu/|\mu|)(x - \overline{\mu}/|\mu|)$. Thus we may assume that the complex roots are on the unit circle. The two cases are given in the following table.

Proposition 9 *Each linear equivalence class of smooth real elliptic curves has an affine Weierstrass model (normal form) as in the following table.*

Table 1

Type	*equation*	*restriction*	*j-invariant*
I	$y^2 = x(x-1)(x-\lambda)$	$0 < \lambda < 1$	$j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$
II	$y^2 = x(x-e^{i\theta})(x-e^{-i\theta})$ $y^2 = x(x^2 - 2\cos(\theta)x + 1)$ $y^2 = x(x^2 - 2bx + 1)$	$0 < \theta < \pi$ $-1 < b < 1$	$j(e^{i2\theta}) = 128\frac{(2\cos(2\theta)-1)^3}{\cos(2\theta)-1}$ $j(b) = 128\frac{(4b^2-3)^2}{b^2-1}$

5 The real moduli space in complex moduli space

Proposition 10 *For all real elliptic curves E the j-invariant $j(E)$ is real, and all real numbers are realized. A real elliptic curve has a single component if and only if $j(E) \leq 1728$ and has two components if and only if $j(E) \geq 1728$.*

Proof. From the form of the j-invariant it is clear that it is real in all cases. That all real numbers are realized will follow from the remainder of the proof. Let us consider Type I. We just need to prove that $j(\lambda)$ sweeps out the range $[1728, +\infty)$. The plot of $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ is given in Figure 1. We have the limits $\lim_{\lambda\to 0} j(\lambda) = \lim_{\lambda \to 1} j(\lambda) = +\infty$, and derivative

$$j'(\lambda) = 256\frac{(\lambda^2-\lambda+1)^2(2\lambda-1)(\lambda+1)(\lambda-2)}{\lambda^3(\lambda-1)^3}.$$

It follows that in the given interval the minimum can only occur at $\lambda = 1/2$ with minimum value of 1728.

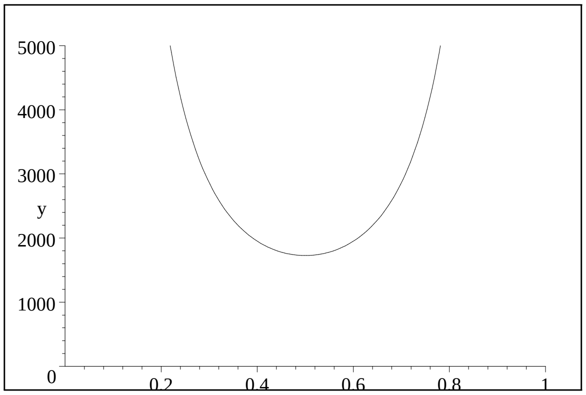

Fig 1. j-invariant in the real Case I

For Type II we need to prove that $j(e^{i2\theta})$ sweeps out the range $(-\infty, 1728]$. The plot of $k(e^{i2\theta})$ $=128\frac{(2\cos(2\theta)-1)^3}{\cos(2\theta)-1}$ is given in Figure 2. We have the limits $\lim_{\theta\to 0} j(e^{i2\theta}) = \lim_{\theta\to\pi} j(e^{i2\theta}) = -\infty$, and we have

$$\frac{d}{d\theta} j(e^{i2\theta}) = 128 \frac{(2\cos(2\theta)-1)^2(4\cos(2t)-5)\sin(2t)}{(\cos(2\theta)-1)^2}.$$

The maximum can only occur when $\sin(2\theta) = 0$ or $\theta = \pi/2$,with a maximum value of 1728.

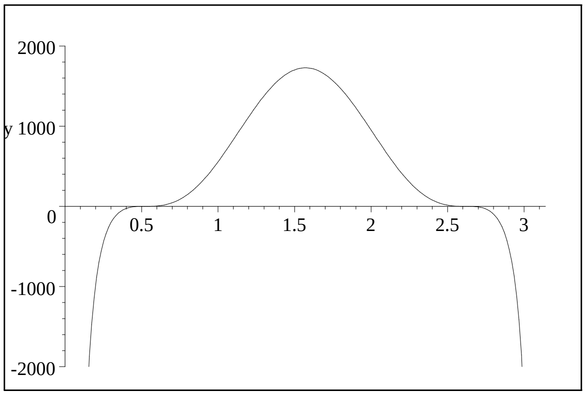

Fig 2. j-invariant in the complex Case II

■

6 Real forms and real birational isomorphism

If $Y_{\mathbb{C}}$ is a projective variety with real defining equations then there is an anti-holomorphic involution σ_0 with of $Y_{\mathbb{C}}$ with fixed point set $Y_{\mathbb{R}}$. The involution is defined by complex conjugation $\sigma_0 : (X_0 : X_1 : \cdots : X_n) \to (\overline{X_0} : \overline{X_1} : \cdots : \overline{X_n})$ of the coordinates of the ambient projective space in which $Y_{\mathbb{C}}$ lies. Now let X be any projective variety. A *symmetry* or *complex conjugation* of X is defined to be any anti-holomorphic self-mapping of order 2 created as follows. Map $\varphi : X \to Y_{\mathbb{C}} \subseteq P^n(\mathbb{C})$ by a birational isomorphism to a variety $Y_{\mathbb{C}}$ defined over $\mathbb{R}$ and pull back the canonical symmetry, i.e., set $\sigma = \varphi^{-1}\sigma_0\varphi$ (see Remark 13 below). Observe that under our construction of σ the real points $Y_{\mathbb{R}}$ of $Y_{\mathbb{C}}$ correspond to the fixed point set $X_\sigma = \{x \in X : \sigma(x) = x\}$ under φ. Thus there is a 1-1 correspondence between real defining equations of X (up to real birational equivalence) and the symmetries of X. The various fixed point sets of symmetries are called the real forms of X. By considering symmetries of X we can capture all the real forms of X at once in the context of the automorphism group of X. This is made explicit by the following proposition.

Proposition 11 *Let X be a complex projective variety X defined over $\mathbb{R}$. Let Aut(X) denote the group of birational (holomorphic) automorphisms of X, τ some fixed but arbitrary symmetry of X, and σ_1 and σ_2 be two arbitrary symmetries of X. Then we have the following.*

1. For φ in $\mathrm{Aut}(X)$, $\sigma_1\varphi\sigma_2$ is an automorphism of X. Hence, $\sigma_1\sigma_2$ is an automorphism of X, by taking φ to be the identity map.

2. Let $\mathrm{Aut}(X)\tau = \{\varphi\tau : \varphi \in \mathrm{Aut}(X)\}$. Then the set $\mathrm{Aut}^*(X) = \mathrm{Aut}(X) \cup \mathrm{Aut}(X)\tau$ is a group of transformations of X containing $\mathrm{Aut}(X)$ as a subgroup of index 2.

3. Every symmetry of X has the form $\varphi\tau$ where
$$\tau\varphi\tau = \varphi^{-1}. \tag{11}$$
Further, if $\varphi \in \mathrm{Aut}(X)$ then the transformation $\varphi\tau\varphi^{-1}$ is a symmetry of X.

4. The real forms X_{σ_1} and X_{σ_2} of X are (ambiently) birationally isomorphic over $\mathbb{R}$ if and only if $\sigma_2 = \varphi\sigma_1\varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(X)$. Thus the real forms of X are in 1-1 correspondence with the $\mathrm{Aut}(X)$-conjugacy classes of symmetries of X.

Proof.

1. Suppose that $\sigma_1 = \varphi_1^{-1}\sigma_0\varphi_1$ and $\sigma_2 = \varphi_2^{-1}\tau_0\varphi_2$ where σ_0 and τ_0 are canonical involutions on possibly different projective spaces. Then
$$\begin{aligned} \sigma_1\varphi\sigma_2 &= (\varphi_1^{-1}\sigma_0\varphi_1)\varphi(\varphi_2^{-1}\tau_0\varphi_2) \\ &= \varphi_1^{-1}(\sigma_0\varphi_1\varphi\varphi_2^{-1}\tau_0)\varphi_2 \end{aligned}$$
It is not hard to show that $\sigma_0\varphi_1\varphi\varphi_2^{-1}\tau_0$ is the rational morphism obtained by conjugating the coefficients, but not the variables in the formula for $\varphi_1\varphi\varphi_2^{-1}$. Hence $\sigma_1\varphi\sigma_2$ is a rational map. It is bijective since its factors are bijective.

2. It follows from statement 1 that $\mathrm{Aut}(X)\cup$ $\mathrm{Aut}(X)\tau$ is closed under multiplication. Since $\mathrm{Aut}(X)\cap$ $\mathrm{Aut}(X)\tau$ is empty, because a map is not simultaneously holomorphic and anti holomorphic, $\mathrm{Aut}(X)$ is a subgroup of index 2.

3. If σ is any symmetry of X then $\sigma = \sigma(\tau\tau) = (\sigma\tau)\tau$, with $\sigma\tau \in\mathrm{Aut}(X)$ by statement 2. Now $\sigma = \varphi\tau$ and $id = \sigma^2 = \varphi\tau\varphi\tau$. It follows that $\tau\varphi\tau = \varphi^{-1}$. The rest of Statement 4 is left to the reader.

4. Suppose that $\sigma_1 = \varphi_1^{-1}\sigma_0\varphi_1$ and $\sigma_2 = \varphi_2^{-1}\tau_0\varphi_2$ for maps $\varphi_1 : X \to Y_{\mathbb{C}} \subseteq P^{n_1}(\mathbb{C})$ and $\varphi_2 : X \to Z_{\mathbb{C}} \subseteq P^{n_2}(\mathbb{C})$ as in the proof of statement 1 above. Now suppose that in addition $\sigma_2 = \varphi\sigma_1\varphi^{-1}$ for some $\varphi \in\mathrm{Aut}(X)$. Then $\varphi(X_{\sigma_1}) = X_{\sigma_2}$ and $\psi = \varphi_2\varphi\varphi_1^{-1}$ maps $Y_{\mathbb{C}} \to Z_{\mathbb{C}}$ carrying $Y_{\mathbb{R}} \to Z_{\mathbb{R}}$. It is sufficient to show that $\varphi_2\varphi\varphi_1^{-1}$ is a real rational mapping. As discussed in the proof of Statement 1 the map $\tau_0\varphi_2\varphi\varphi_1^{-1}\sigma_0$ is the same as the map $\varphi_2\varphi\varphi_1^{-1}$ except that all the coefficients have been replaced by their complex conjugates. Thus we need only show that

   $$\tau_0\varphi_2\varphi\varphi_1^{-1}\sigma_0 = \varphi_2\varphi\varphi_1^{-1}.$$

   Our conjugacy hypothesis can be written $\sigma_2\varphi = \varphi\sigma_1$ or

   $$\varphi_2^{-1}\tau_0\varphi_2\varphi = \varphi\varphi_1^{-1}\sigma_0\varphi_1$$

   or

   $$\tau_0\varphi_2\varphi\varphi_1^{-1} = \varphi_2\varphi\varphi_1^{-1}\sigma_0$$

   Thus

   $$\tau_0\varphi_2\varphi\varphi_1^{-1}\sigma_0 = \varphi_2\varphi\varphi_1^{-1}\sigma_0\sigma_0 = \varphi_2\varphi\varphi_1^{-1}.$$

   Now suppose that there is a birational isomorphism $\psi : Y_{\mathbb{C}} \to Z_{\mathbb{C}}$ which is defined over $\mathbb{R}$ and maps $Y_{\mathbb{R}} \to Z_{\mathbb{R}}$ isomorphically. Because the map is real then $\tau_0\psi\sigma_0 = \psi$. In the previous part of the proof we had $\psi = \varphi_2\varphi\varphi_1^{-1}$ so let us try $\varphi = \varphi_2^{-1}\psi\varphi_1$ for our conjugating map. We need to show that $\sigma_2 = \varphi\sigma_1\varphi^{-1}$ or $\sigma_2\varphi\sigma_1\varphi^{-1} = id$. Now

   $$\begin{aligned} \sigma_2\varphi\sigma_1\varphi^{-1} &= (\varphi_2^{-1}\tau_0\varphi_2)(\varphi_2^{-1}\psi\varphi_1)(\varphi_1^{-1}\sigma_0\varphi_1)(\varphi_1^{-1}\psi^{-1}\varphi_2) \\ &= \varphi_2^{-1}\tau_0\psi\sigma_0\psi^{-1}\varphi_2 = \varphi_2^{-1}\psi\psi^{-1}\varphi_2 = id. \end{aligned}$$

■

Remark 12 *It is possible that the real form X_σ is empty. E.g., the complexification of the variety defined by $x^2 + y^2 = -1$ has empty real form. On the other hand $x^2 - y^2 = 1$ $((x, y) \to (ix, y))$ and $x^2 + y^2 = 1$ $((x, y) \to (ix, iy))$ are other real forms which are not empty.*

Remark 13 *More generally, a* symmetry *or* complex conjugation *of a projective variety X is defined to be any anti-holomorphic self mapping of order 2. Under this more general definition the symmetries are all elements of $Aut(X)\tau$*

which satisfy $\tau\varphi\tau = \varphi^{-1}$, and are easily identified if the group is known. In the case of curves general symmetries and symmetries created by pullback are the same. However our restricted definition is sufficient.

Remark 14 *For elliptic curves the automorphism group is infinite and transitive on the curve, more precisely the real automorphism group is transitive on the real part and the complex automorphism group is transitive on the complex curve. Once we fix the base point at infinity, by assuming a Weierstrass form, we may replace the automorphism groups in the forgoing by the groups of automorphisms and symmetries fixing ∞.*

7 Real forms and symmetries of elliptic curves

Because all our curves are in Weierstrass form, we are only going to consider real forms that pass through the base point of the elliptic curve, ∞, i.e., the identity point of the group law. According to the Remark 14 in the last section, we need only consider automorphisms and symmetries that fix this point. It is well known that the automorphism groups of complex elliptic curves, fixing the base point, are as follows, where we have written the equations to make the automorphism groups obvious.

Table 2

Case	equation	j-invariant	Aut(E) and generator
I	$y^2 = x(x^2-1)$	1728	$\mathbb{Z}_4$, $(x,y) \to (-x, iy)$
II	$y^2 = x^3 - 1$	0	$\mathbb{Z}_6$, $(x,y) \to (\omega x, -y)$, $\omega = \exp(2\pi i/3)$
III	$y^2 = x(x-\lambda_1)(x-\lambda_2)$	all other reals	$\mathbb{Z}_2$, $(x,y) \to (x,-y)$

The real forms are as follows:

Table 3

Case	equation	j-invariant	real forms
I	$y^2 = x(x^2-1)$	1728	$y^2 = x(x^2-1)$ $y^2 = x(x^2+1)$
II	$y^2 = x^3 - 1$	0	$y^2 = x^3 - 1$ $y^2 = x^3 + 1$
III	$y^2 = x(x-\lambda_1)(x-\lambda_2)$	all other reals	$y^2 = \pm x(x-\lambda_1)(x-\lambda_2)$

The real forms can be found by the following general procedure. Pick τ to be standard complex conjugation $\tau : (x,y) \to (\overline{x}, \overline{y})$ in the affine plane. Now assume that an automorphism φ is given by an affine linear transformation. Find another linear transformation ψ, which need not fix E such that $\varphi\tau = \psi\tau\psi^{-1}$. Then $\psi(E_{\mathbb{R}})$ is a real form corresponding to $\varphi\tau$.

Let us demonstrate this by working out the examples in the table. Every elliptic curve has the following automorphism. $\varphi : (x,y) \to (x,-y)$, $\varphi\tau$ is

$(x,y) \to (\overline{x}, -\overline{y})$, let us now prove it is a symmetry. Next, set $\psi : (x,y) \to (x, iy)$, then $\varphi\tau = \psi\tau\psi^{-1}$, and so $\varphi\tau$ is a symmetry. Making the substitution $(x,y) \to (x,iy)$ transforms $y^2 = g(x)$ to $y^2 = -g(x)$. More generally, suppose that φ is the monomial transformation $(x,y) \to (\alpha x, \beta y)$ Then the symmetry condition 11 is given by

$$(\overline{\alpha}x, \overline{\beta}y) = (\alpha^{-1}x, \beta^{-1}y),$$

This condition holds if and only if α and β are complex numbers of unit modulus. Seeking a ψ of similar form, set $\psi : (x,y) \to (\gamma x, \delta y)$. With $\varphi\tau = \psi\tau\psi^{-1}$ we get

$$(\alpha\overline{x}, \beta\overline{y}) = (\gamma\overline{\gamma^{-1}}x, \delta\overline{\delta^{-1}}y).$$

Assuming γ and δ to also be of unit modulus we get the equations $\gamma^2 = \alpha$ and $\delta^2 = \beta$. Thus in every case the entire set $\mathrm{Aut}(X)\tau$ consists of symmetries. But how many real forms are there? By statement 4 of Proposition 11 we need to determine the $\mathrm{Aut}(X)$-conjugacy classes of $\mathrm{Aut}(X)\tau$. Observing that $\tau\psi\tau = \psi^{-1}$ for all $\psi \in \mathrm{Aut}(X)$, then,

$$\psi\varphi\tau\psi^{-1} = \psi\varphi\psi\tau = \psi^2\varphi\tau.$$

The set $H = \{\varphi^2 : \varphi \in \mathrm{Aut}(X)\}$ is a subgroup of index 2 and so the conjugacy classes are in 1-1 correspondence to the cosets of H in $\mathrm{Aut}(X)$. Thus there are two real forms for complex elliptic curves defined over $\mathbb{R}$. In every case except $j = 1728$, the inversion automorphism $\varphi : (x,y) \to (x,-y)$ is not a square, therefore it follows for all these curves that $y^2 = g(x)$ and $y^2 = -g(x)$ are non-equivalent real forms.

Now let us consider the two special cases. In the Case I $\varphi : (x,y) \to (x,-y)$ is a square in $\mathrm{Aut}(X)$ so $y^2 = -g(x)$ will not be a distinct real form. However the generator of $\mathrm{Aut}(X)$ is not a square. Applying the method in above with $\gamma = i$ and $\delta = \exp(i\pi/4)$ the substitution $(x,y) \to (\gamma x, \delta y)$ takes $y^2 = x(x^2-1)$ to $y^2 = x(x^2+1)$. For Case II, we have listed a different form of the real equations to make the automorphisms obvious. To get to the standard forms of equation with $\theta = \pi/12$, $11\pi/12$, apply the transformation $y^2 - g(x) \to \frac{1}{\sqrt{27}}((\sqrt[4]{27}y)^2 - g(\sqrt{3}x+1))$ to convert $y^2 = x^3 - 1$ to $y^2 = x(x^3 + \sqrt{3}x + 1)$, and $(x,y) \to (\sqrt{3}x - 1, \sqrt[4]{27}y)$, $y^2 - g(x) \to \frac{1}{\sqrt{27}}((\sqrt[4]{27}y)^2 - g(\sqrt{3}x - 1))$ to convert $y^2 = x^3 + 1$ to $y^2 = x(x^3 - \sqrt{3}x + 1)$.

8 The birational isomorphism types of real elliptic curves

Theorem 15 *The birational isomorphism types of real elliptic curves areas are as given in Table 1.*

Proof. All real elliptic curves must occur in the two families listed. If two real elliptic curves are isomorphic, then their complexifications are also isomorphic, and hence their j-invariants are the same. Thus it suffices to show that any two curves listed with the different j-invariant are not isomorphic. First observe that none of the curves in the first group are isomorphic to those in the second group because of a component count. First we consider isomorphism between curves of Type I. Assume that our curves have the equations $y^2 = x(x-1)(x-\lambda)$ $y^2 = x(x-1)(x-\lambda')$, with $0 < \lambda, \lambda' < 1$. According to the condition 2 we must have $\lambda' = 1-\lambda$, as suggested by Figure 1. Indeed, the J-group maps the interval $(0,1)$ to itself, $(1,+\infty)$ and $(-\infty,0)$ with exactly two mappings fixing each interval. The substitution $(x,y) \to (1-x,y)$ takes the equation $y^2 = x(x-1)(x-\lambda)$ to $y^2 = -x(x-1)(x-\lambda')$. Thus $E^\lambda_{\mathbb{R}}$, $E^{\lambda'}_{\mathbb{I}}$ and $E^\lambda_{\mathbb{I}}$, $E^{\lambda'}_{\mathbb{R}}$ are pairwise isomorphic. If $E^\lambda_{\mathbb{R}}$ and $E^{\lambda'}_{\mathbb{R}}$ were isomorphic then there would be an automorphism φ of $E^\lambda_{\mathbb{C}}$ which would conjugate the symmetry defined by $E^\lambda_{\mathbb{R}}$ to that defined by $E^\lambda_{\mathbb{I}}$. However the two symmetries are $\sigma_0 : (x,y) \to (\overline{x},\overline{y})$ for $E^\lambda_{\mathbb{R}}$ and $\sigma_1 : (x,y) \to (\overline{x},-\overline{y})$ for $E^\lambda_{\mathbb{I}}$. For all $\lambda \neq \frac{1}{2}$ under consideration $E^\lambda_{\mathbb{C}}$ has a single non-trivial automorphism $\varphi : (x,y) \to (x,-y)$ fixing ∞, which satisfies $\varphi\sigma_0\varphi^{-1} = \sigma_0$. Thus $E^\lambda_{\mathbb{R}}$ and $E^{\lambda'}_{\mathbb{R}}$ are not real isomorphic.

Now assume the equation of our curve is $y^2 = x(x-e^{i\theta})(x-e^{-i\theta})$, $y^2 = x(x^2-2\cos(\theta)x+1)$. The j-invariant is $j(e^{2i\theta})$. The values of the cross-ratio $e^{2i\theta}$ sweep out the unit circle minus the point 1. The $J-$group again maps this set to itself, the unit circle centered at $1/2$ and the vertical line $x = 1/2$. There are exactly two mappings carrying each set to itself. The three curves intersect at the parameter value corresponding to a special curve with extra automorphisms. For points in the unit circle two points $\lambda = e^{2i\theta}$ and $\lambda' = e^{2i\theta'}$ will have the same j-invariant if and only if $\lambda' = 1/\lambda$, i.e. $\theta' = \pi - \theta$ as suggested by Figure 2. The transformation $(x,y) \to (-x,y)$ takes the equation $y^2 = x(x^2-2\cos(\theta)x+1)$ to $y^2 = -x(x^2+2\cos(\theta)x+1)$, i.e., $y^2 = -x(x^2-2\cos(\theta')x+1)$. The remainder of the proof for this case is exactly as in the previous case. ■

The analysis in Section 7 proves the following

Proposition 16 *The elliptic curve with four symmetries and* $j = 1728$ *is the only elliptic curve where the real forms may have a different number of components. It is the intersection of the "real" and the "imaginary" curves.*

Proposition 17 *Two smooth real elliptic curves in* $P^2(\mathbb{C})$ *are birationally isomorphic if and only if the are linearly isomorphic.*
Proof. *Table 1 was constructed by selecting at least one linear isomorphism type for every smooth real curve. If there were duplication among the set then two curves would be birationally isomorphic. However, this contradicts Theorem 15* ■

References

[1] David Mumford, *Curves and Their Jacobians*, University of Michigan Press, Ann Arbor, (1976).