MODULI SPACE OF REAL GENUS ONE CURVES

In a previous write-up, we derived the picture in Figure 1, which depicts the moduli space of real elliptic curves, up to real isomorphism. We now wish to extend that picture to include all genus one curves over $\mathbb{R}$.

Every genus one curve C/k with $C(k) \neq \emptyset$ can be described by a Weierstrass equation:

$$y^2z = x^3 + fxz^2 + gz^3$$

Analogously, every genus one curve C/k with $C(k(\sqrt{a})) \neq \emptyset$ can be described by a an equation:

$$C : w^2 = au^4 + bu^3v + cu^2v^2 + duv^3 + ev^4$$

Since every genus one curve over $\mathbb{R}$ is guaranteed to have a point over a quadratic extension, we can study all genus one curves over $\mathbb{R}$ by studying curves of the form $w^2 = q(u, v)$, where $q(u, v)$ is a binary quartic.

The Jacobian of the genus one curve $C/\mathbb{R}$ above is the elliptic curve:

$$Jac(C): \quad y^2 = x^3 + f(C)x + g(C)$$

$$f(C) = \frac{3bd - c^2 - 12ae}{3} \qquad g(C) = \frac{2c^3 - 9bcd + 27(ad^2 + b^2e) - 72ace}{27}$$

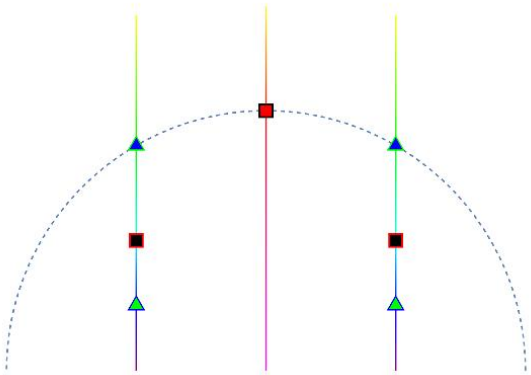

FIGURE 1. Moduli space of real elliptic curves. Points of the same color represent $\mathbb{R}$-isomorphic elliptic curves. The points labelled with a square represent elliptic curves with $j = 1728$, and those labelled with a triangle represent elliptic curves with $j = 0$.

If $C(\mathbb{R}) \neq \emptyset$, then $C, Jac(C)$ are isomorphic as real algebraic curves. We write $j(C)$ for the j-invariant of $Jac(C)$.

If q is a quartic, we write C_q for the genus one curve $w^2 = q(u, v)$. We also define $f(q) = f(C_q), g(q) = g(C_q), j(q) = j(C_q)$. Let $G = SL_2(\mathbb{R}), \gamma \in G$, q a quartic and define:

$$(\gamma \cdot q)(u, v) = q(\gamma_{11}u + \gamma_{12}v, \gamma_{21}u + \gamma_{22}v)$$

An easy computation shows that:

$$f(q) = f(\gamma \cdot q) \quad g(q) = g(\gamma \cdot q)$$

so $Jac(C_q) = Jac(C_{\gamma \cdot q})$. We say that q, q' are G-equivalent if $\gamma \cdot q = q'$ for some $\gamma \in SL_2(\mathbb{R})$.

Since space of quartics is 5-dimensional and G is 3-dimensional, we can use the action of G to reduce to 2-dimensional parameter spaces. We will implicitly be using the Iwasawa decompostion to eliminate degrees of freedom one by one. We will then use j-invariant to distinguish between non-isomorphic points in our smaller parameter space.

Important Remark: Let $\lambda \in \mathbb{R}^\times$ and q a quartic. The quartics $q, \lambda q$ are not G-equivalent in general, but the associated genus one curves are $\mathbb{R}$-isomorphic if $\lambda > 0$ (the isomorphism given by $w \mapsto \sqrt{\lambda} w$), and they are quadratic twists otherwise.

1. Non-split Quartics

1.1. **Quadratic Forms.** Every quartic form over $\mathbb{R}$ can be factored as a product (in a non-unique way) as a product of real quadratic forms. Since quadratic forms are much easier to study than quartic forms, we will exploit this fact to make headway on the problem.

Write $\mathcal{S}_2 = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ for the space of symmetric 2×2 matrices. We identify $\mathcal{S}_2$ with the space of binary quadratic forms by associating to a symmetric matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ the quadratic form $q(u, v) = au^2 + 2buv + cv^2$. We write q to denote generic elements of $\mathcal{S}_2$ when viewing them as quadratic forms, and M_q for the associated matrix. We write q_0 for the quadratic form associated to the identity matrix, We say that q is isotropic if there exists $(u, v) \in \mathbb{R}^2 - \{(0, 0)\}$ with $q(u, v) = 0$, and anisotropic otherwise.

We define an action of $G = SL_2(\mathbb{R})$ on $\mathcal{S}_2$ by $\gamma \cdot M_q = \gamma^t M_q \gamma$ - an easy computation shows that $\gamma \cdot M_q$ is symmetric if M_q is symmetric. At the level of quadratic forms, this corresponds to replacing $q(u, v)$ by $q(\gamma \cdot (u, v))$, so this action is compatible with G-equivalence

of quadratic forms. Let K, A, N be the subgroups:

$$K = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \right\} \qquad A = \left\{ \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \right\} \qquad N = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right\}$$

Lemma 1.1. *Let $q(u,v) = au^2 + 2buv + cv^2$. We say that q is diagonal if $b = 0$ and q is balanced if $|a| = |c|$. If $a \neq 0$, then:*

(1) *There exists $\kappa \in K$ such that $\kappa \cdot q(u,v)$ is diagonal.*
(2) *There exists a unique $\nu \in N$ such that $\nu \cdot q$ is diagonal.*
(3) *There exists $\alpha \in A$ such that $\alpha \cdot q$ is balanced.*

Proof. Claim (1) is nothing more than the spectral theorem for real symmetric matrixes.

To prove claim (2), let $\nu_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in N$ and compute:

$$\nu_t \cdot q(u,v) = au^2 + 2(at+b)uv + (at^2 + 2bt + c)v^2$$

Thus, $\nu_t \cdot q$ is diagonal precisely when $t = -\frac{b}{a}$.

Finally, to prove claim (3), set $\alpha_r = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$. Then:

$$\alpha_r \cdot q(u,v) = r^2 au^2 + buv + r^{-2}cv^2$$

Let $\varepsilon_a = \frac{a}{|a|}$, $\varepsilon_c = \frac{c}{|c|}$ and $\rho = (a^{-1}c)^{1/4}$. Then:

$$\alpha_\rho \cdot q(u,v) = \varepsilon_a \sqrt{|ac|}u^2 + buv + \varepsilon_c \sqrt{|ac|}v^2$$

Since $|\varepsilon_a| = |\varepsilon_c| = 1$, $\alpha_\rho \cdot q$ is balanced, proving (3).

□

Now, let $\nu \in N$ and let $q_a(u,v) = a(u^2+v^2)$ for some $a \in \mathbb{R}$. An easy computation shows that $\nu \cdot q_a(u,v) = q_a(u,v)$:

$$\begin{aligned}(\nu \cdot q)(u,v) &= a((\cos\theta u + \sin\theta v)^2 + (-\sin\theta u + \cos\theta v)^2 \\ &= a((\cos^2\theta + \sin^2\theta)u^2 + 2(\cos\theta\sin\theta - \sin\theta\cos\theta)uv + (\sin^2\theta + \cos^2\theta)v^2) \\ &= a(u^2+v^2) \\ &= q_a(u,v)\end{aligned}$$

We now put it all together to prove the following:

Proposition 1.2. *Let $q(u,v)$ be a real binary quartic. Then either $q(u,v)$ splits completely, or $q(u,v)$ is equivalent to a quartic of the form:*

$$(u^2+v^2)(au^2+bv^2)$$

for some $a, b \in \mathbb{R}$.

Proof. Choose a factorization of q into quadratic forms $q(u,v) = p_1(u,v)p_2(u,v)$. If q does not split completely, then at least one of p_1, p_2 is irreducible; WLOG assume that p_2 is irreducible.

- First, we find an element $\nu \in N$ that diagonalizes p_2. We act on q by that element to obtain a new, factored quartic where the second factor is irreducible and diagonalized.
- Next, we act on the new q by an element of αA so that p_2 is balanced. Since the action of A takes diagonal forms to diagonal forms, we now have a second factor which is balanced, diagonal and irreducible, i.e. it is a scalar multiple of u^2+v^2. Absorbing the scalar into $p_1(u,v)$, we may assume that the new q has the form $p_1(u,v)(u^2+v^2)$.
- Finally, we can find $\kappa \in K$ that diagonalizes p_1. Acting on q by κ fixes the second factor and diagonalizes the first, so we've obtained a new quartic of the form:

  $$q(u,v) = (au^2+bv^2)(u^2+v^2)$$

  as desired.

□

This shows that every quartic which does not split completely is equivalent, after a change of basis, to a quartic of the form $(au^2+bv^2)(u^2+v^2)$. This includes all quartics that give rise to genus one curves without an $\mathbb{R}$-point, as well as all genus one curves with $j < 1728$.

1.2. **j-invariants.** For $a, b \in \mathbb{R}$, we define:

$$q_{a,b}(u,v) = (au^2+bv^2)(u^2+v^2)$$

Note that $q_{a,b}$ is nondegenerate iff $ab(a-b) \neq 0$. Let $\mathcal{A} = \{(a,b) \in \mathbb{R}^2 : ab(a-b) \neq 0\}$; we will think of $(a,b) \in \mathcal{A}$ as representing $q_{a,b}$.

Let $j : \mathcal{A} \to \mathbb{R}$ be the map that sends (a,b) to the j-invariant of the Jacobian of the genus one curve $w^2 = q_{a,b}(u,v)$. Using standard computations in invariant theory, we can obtain an explicit formula for $j(a,b)$:

$$j(a,b) = 16 \cdot \frac{(a^2+14ab+b^2)^3}{ab(a-b)^4}$$

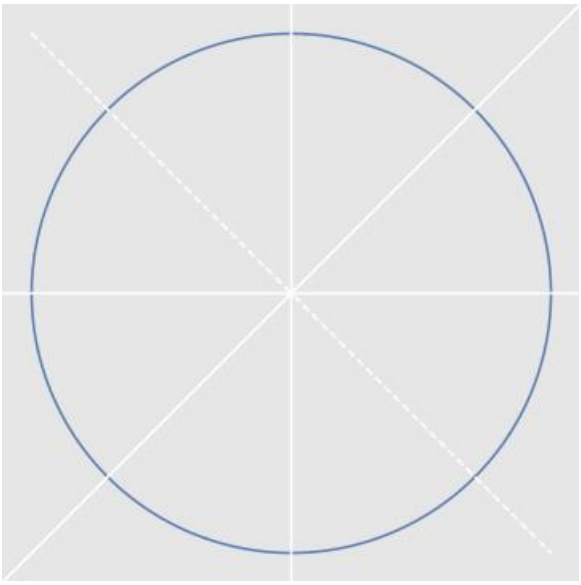

FIGURE 2. Parameter space for quartics with an irreducible factor. Quartics on the dashed line have j-invariant 1728. Reflecting about the dashed line represents quadratically twisting the associated genus one curves.

- Since $j(a,b)$ is a ratio of homogenous sextics in a, b, it is constant along scalar multiples - that is, $j(a,b) = j(\lambda a, \lambda b)$ for all $\lambda \in \mathbb{R}^\times$. Thus, the entire behavior of j is encoded in the behavior of j on the unit circle.

  Note that genus one curves without a real point are represented by points $(a,b) \in \mathcal{A}$ with $a < 0$ and $b < 0$. If we replace (a,b) with $(-a,-b)$, the genus one curve we obtain has the same j-invariant, but now has points defined over $\mathbb{R}$.
- It's also easy to see that $j(a,b) = j(b,a)$. Since:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot q_{a,b}(u,v) = q_{a,b}(-v,u) = (av^2 + bu^2)(v^2 + u^2) = q_{b,a}(u,v)$$

  the points $(a,b), (b,a) \in \mathcal{A}$ represent isomorphic genus one curves.

Thus, we should be able to find a fundamental domain in Figure 2.

The next step is checking that we have the right number of isomorphism class for each $j \in \mathbb{R}$.

- First, it's easy to see that $j(a,b) = 0$ iff $a^2 + 14ab + b^2 = 0$. There are two solutions two that quadratic in $\mathbb{P}^1_{\mathbb{R}}$, giving us 4 solutions in $\mathcal{A}/\mathbb{R}^+$. The $(a,b) \leftrightarrow (b,a)$ symmetry gives us two solutions, up to isomorphism of genus one curves.

  This is the number we expected: there are exactly 2 isomorphism classes of elliptic curves with $j = 0$.

- Next, we compute $j^{-1}(1728)$. The sextic polynomial:

$$j(a,b) = 1728 \quad \iff \quad 16(a^2+14ab+b^2) - 1728ab(a-b)^4 = 0$$

We can factor the sextic as:

$$16(a^2+14ab+b^2) - 1728ab(a-b)^4 = 16(a+b)^2(a^2-34ab+b^2)^2$$

This gives us 3 roots in $\mathbb{P}^1$.

Note that $q_{1,-1} = q_{-1,1}$, so we don't need to count $(1,-1),(-1,1)$ separately. The other two roots each correspond rise to two distinct quartics, but we end up identifying them in pairs due to the $(a,b) \leftrightarrow (b,a)$ symmetry.

Altogether, we have exactly 3 isomorphism classes of quartics with $j = 1728$, which again is exactly the number we expected.

- Define $J(a,b,t) = 16(a^2+14ab+b^2)^3 - tab(a-b)^4$. The discriminant of $J(a,b,t)$, viewed as a binary sextic in a, b, is:

$$-72057594037927936(-1728+t)^3t^4$$

Thus, for any $t_0 \neq 0, 1728$, $J(a,b,t_0) = 0$ is locally invertible, so in particular, the number of real solutions is locally constant.

By computing an example in each connected component, we find that the number of distinct quartics $q_{a,b}$ with $j(a,b) = j_0 > 1728$ is 4, and the number of (a,b) with $j(a,b) = j_0 < 1728$ is 2.

This gives us the picture in Figure 3.

Since some of the features are hard to see on that picture, it is also helpful to look at the following topologically equivalent picture in Figure 4.

Thus, the picture above contains exactly the right number of isomorphism classes for every $j \in \mathbb{R}$! This is somewhat surprising, as we have not yet done anything with quartics that split completely. Nevertheless, we can now extend our previous picture of the moduli space of real elliptic curves to now include a unique representative for all real genus one curves over $\mathbb{R}$.

2. Totally Split Quartics

Although we've accomplished the goal stated at the beginning, the story doesn't feel complete, since we never considered quartics that split completely. We discuss those now.

Let $q(u,v)$ be a quartic that splits completely. Replacing $q(u,v)$ by $q(u,\varepsilon u+v)$ if necessary, we may assume that $q(u,1)$ has nonzero leading coefficient, so it has 4 real roots. We denote these by $\rho_1, \rho_2, \rho_3, \rho_4$, with the roots indexed so $\rho_i < \rho_j$ if and only if $i < j$.

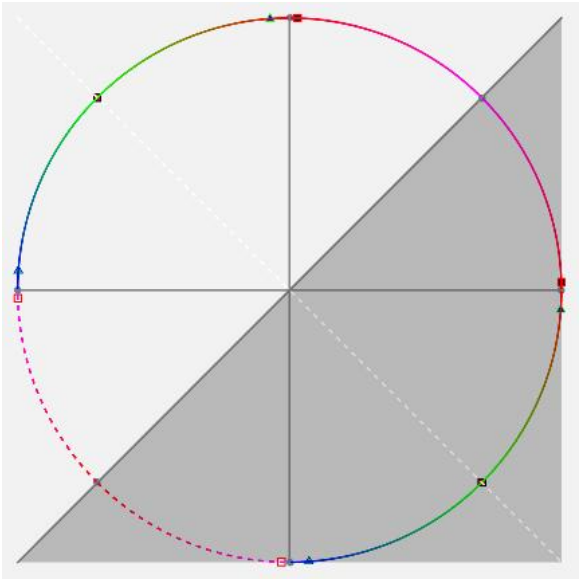

FIGURE 3. Space of genus one curves over $\mathbb{R}$, up to $\mathbb{R}$-isomorphism, in the (a, b)-plane. The picture is drawn to scale.

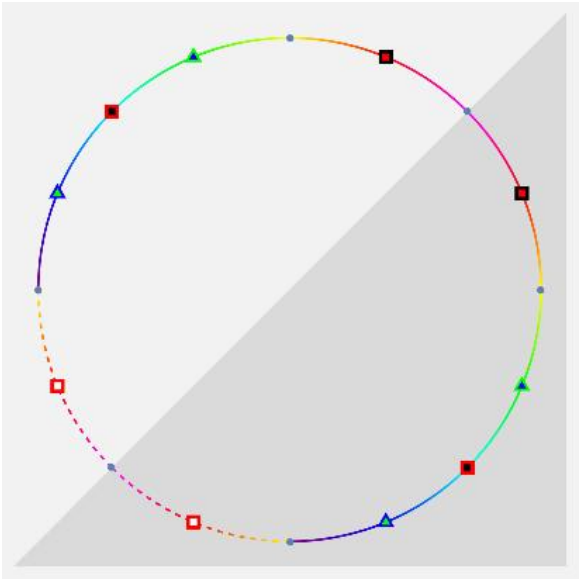

FIGURE 4. Space of genus one curves over $\mathbb{R}$, up to $\mathbb{R}$-isomorphism, not drawn to scale.

Let T be the automorphism:

$$T : \mathbb{P}^1 \to \mathbb{P}^1 \qquad T(x) = \frac{x - \rho_3}{x - \rho_1}$$

Observe that $T(\rho_2) < 0$ and $T(\rho_4) > 0$.

Let $\gamma_T \in GL_2(\mathbb{R})$ be the matrix $\begin{pmatrix} 1 & -\rho_3 \\ 1 & -\rho_1 \end{pmatrix}$. Rescaling one of the rows of γ_T if necessary, we may assume $\gamma_T \in SL_2(\mathbb{R})$. Let $\gamma = \gamma_T^{-1}$.

Then $\gamma \cdot q(u, 1)$ is a 1-variable cubic in u with a root at 0, a positive root and a negative root (the fourth root is at infinity). Thus, we can factor the new polynomial as:

$$(\gamma \cdot q)(u, v) = uv(a_1u + b_1v)(a_2u + b_2v) = uv(a_1a_2u^2 + (a_1b_2 + a_2b_1)uv + b_1b_2v^2)$$

where $a_1b_1 < 0$ and $a_2b_2 > 0$. Note that this means $a_1a_2b_1b_2 < 0$.

To summarize, we've shown that every quartic that splits completely is equivalent to a quartic of the form:

$$q(u, v) = uv(au^2 + buv + cv^2)$$

where a, c have different signs.

Now, recall that we can act on a binary quadratic form by a matrix of the form $\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$ to obtain an equivalent quadratic form which is balanced, i.e. where $|a| = |c|$. Furthermore, uv is fixed by that action, so we can eliminate an additional parameter by balancing the second factor of $q(u, v)$ to obtain a quartic:

$$q^s_{a,b}(u, v) = uv(au^2 + buv - av^2)$$

We have now reduced the parameter space to a 2-dimensional subset. Acting on $q^s_{a,b}$ by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ fixes b and negates a, so we will be assuming $a > 0$ in the remainder.

Define:

$$j^s(a, b) = j(q^s_{a,b}) = 64\frac{(3a^2 + 4b^2)^3}{a^4(a^2 + b^2)}$$

and:

$$J(a, b, t) = 64(3a^2 + 4b^2)^3 - ta^4(a^2 + b^2)$$

Note that $j^s(a, b) = t$ if and only if $J(a, b, t) = 0$.

Viewing $J(a, b, t)$ as a homogenous sextic in a, b, we can compute the discriminant as a function of t:

$$\Delta(J(a, b, t))(t) = N(t - 1728)^3t^4$$

Thus, on the interval $t \in (1728, \infty)$, the number of solutions to $J(1, b, t) = 0$ is locally constant. Solving $J(1, b, t_0) = 0$ for b at specific examples with $t_0 > 1728$, we find the number of roots is exactly 2 on that interval, and the two roots are negatives of each other. When $b = 0$, the elliptic curve has j-invariant 1728.

The picture is now straightforward:

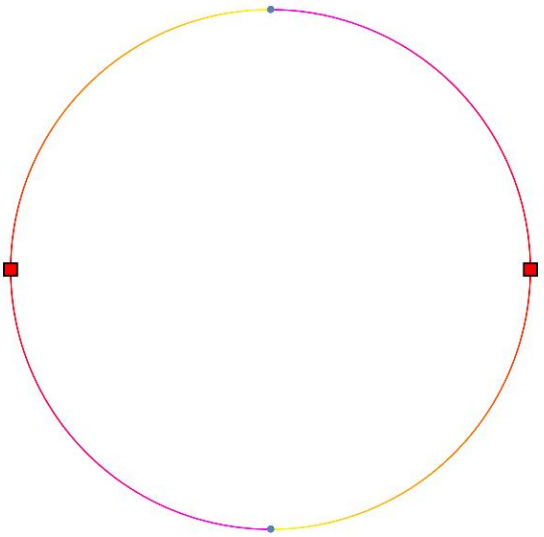

FIGURE 5. Genus one curves associated to totally split quartics.

3. SUMMARY

- Every genus one curve over $\mathbb{R}$ can be written as $w^2 = q(u, v)$ for some quartic.
- If the quartic $q(u, v)$ does not split completely, then $q(u, v)$ is equivalent to a quartic of the form $(au^2 + bv^2)(u^2 + v^2)$ for some $a, b \in \mathbb{R}$. The $\mathbb{R}$-isomorphism classes of genus one curves of this form are depicted in Figures 3,4.
- If the quartic splits completely, then we can do a change of variable so that it has the form $uv(au^2 + buv - av^2)$ with $a > 0$. The $\mathbb{R}$-isomophism classes of genus one curves of this form are depicted in Figure 5.