

THE MODULI SPACE OF ELLIPTIC CURVES OVER \mathbb{R}

Let k be a field. We would like to describe the space of k -isomorphism classes of genus one curves over k . There are several great descriptions when $k = \mathbb{C}$, but they make use of the fact that every genus one curve over \mathbb{C} necessarily has a point defined over \mathbb{C} . Those methods are therefore of very limited use if we want a description of the space when k is a number field, since in that case it can be hard to even decide whether a single curve has any rational points. However, if we take $k = \mathbb{R}$, then the problem is different enough from the classical version that we start to see new phenomena, but not so difficult that we have to invent new methods.

As a warm up, we give an abstract definition of the moduli space of elliptic curves over a field. An elliptic curve is a pair (C, p) consisting of a genus one curve C/k and $p \in C(k)$ a k -rational point. For any (C, p) , we can find an isomorphism $C \rightarrow E$ to a plane curve with an equation:

$$E : y^2z = x^3 + fxz^2 + gz^3 \quad p \mapsto [0 : 1 : 0]$$

Thus, it suffices to classify curves given by an equation of the form above, up to k -isomorphism. If $4f^3 + 27g^2 = 0$, then the equation defines a singular curve, so we take:

$$\mathcal{W}(k) = \{(f, g) \in k^2 : 4f^3 + 27g^2 \neq 0\}$$

as a parameter space for all elliptic curves over k .

For each $(f, g) \in \mathcal{W}(k)$, write:

$$E_{(f,g)} : y^2 = x^3 + fx + g$$

Define an action of k^\times on $\mathcal{W}(k)$ by:

$$t \cdot (f, g) = (t^4f, t^6g)$$

For each $t \in k^\times$, define:

$$\Phi_t : E_{(f,g)} \rightarrow E_{t \cdot (f,g)} \quad (x, y) \mapsto (t^2x, t^3y)$$

Then Φ_t gives an isomorphism between $E_{(f,g)}, E_{t \cdot (f,g)}$ for any $(f, g) \in \mathcal{W}(k)$. Furthermore, this holds for all $t \in k^\times$. One can also show that two elements of $\mathcal{W}(k)$ are k -isomorphic if and only if they lie in the same k^\times orbit, so we obtain a preliminary description of the moduli space as:

$$\mathcal{W}(k)/k^\times$$

Our goal in the subsequent sections is to understand this quotient better, and ultimately to extend it to a space that also classifies genus one curves without a k -point.

1. ELLIPTIC CURVES OVER \mathbb{C}

If $k = \mathbb{C}$, every genus one curve is isomorphic to an elliptic curve, and we know that that the moduli space of elliptic curves is:

$$\mathcal{W}(\mathbb{C})/\mathbb{C}^\times$$

However, we can also describe the moduli space analytically using the theory of Riemann surfaces. Let E be the elliptic curve:

$$y^2 = x^3 + fx + g$$

and define a differential form:

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 - f}$$

Let γ_1, γ_2 be a basis of $H_1(E, \mathbb{Z})$ and define $\omega_i = \int_{\gamma_i} \omega$. The **period lattice** of E is the lattice:

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

If γ, γ' are homologous paths on E , then the difference $\int_\gamma \omega - \int_{\gamma'} \omega$ is an element of Λ .

Now, for each $p \in E(\mathbb{C})$, choose a path $\gamma_p : [0, 1] \rightarrow E$ with $\gamma_p(0) = [0 : 1 : 0]$ and $\gamma_p(1) = p$. We can define a map:

$$E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda \quad p \mapsto \int_{\gamma_p} \omega + \Lambda$$

Since we've taken the quotient by Λ , the value of the integral does not depend on the choice of path, so this map is well-defined and it gives an isomorphism between $E(\mathbb{C})$ and \mathbb{C}/Λ .

Conversely, let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ be a lattice in \mathbb{C} . Set $\Lambda' = \Lambda - \{0\}$. Define:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda'} \frac{1}{(z + \lambda)^2} - \frac{1}{\lambda^2}$$

and, for each $k \geq 1$:

$$g_k(\Lambda) = \sum_{\lambda \in \Lambda'} \frac{1}{\lambda^{2k}}$$

Then \wp_Λ satisfies the differential equation:

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + 60g_2(\Lambda)\wp_\Lambda(z) + 140g_3(\Lambda)$$

so we can define a map $\mathbb{C}/\Lambda \rightarrow E$ to the elliptic curve:

$$E : \quad y^2 = 4x^3 + 60g_2(\Lambda)x + 140g_3(\Lambda)$$

Thus, every Weierstrass equation determines a lattice, and starting from any lattice we can obtain a Weierstrass equation. Replacing a Weierstrass equation by an equivalent one, i.e. replacing $E_{(f,g)}$ by $E_{t \cdot (f,g)}$ replaces the period lattice Λ by $t^{-1}\Lambda$, so every \mathbb{C} -isomorphism class of elliptic curves corresponds to a \mathbb{C} -homothety class of lattices and vice versa.

This leads to the familiar description of the moduli space of elliptic curves with $SL(2, \mathbb{Z}) \backslash \mathcal{H}$:

- Let $\omega_1 \mathbb{Z} \oplus \omega_2 \mathbb{Z}$ be a nondegenerate lattice in \mathbb{C} (i.e. ω_1, ω_2 are \mathbb{R} -linearly independent). Then Λ is homothetic to $\frac{\omega_1}{\omega_2} \mathbb{Z} \oplus \mathbb{Z}$. Since ω_1, ω_2 are \mathbb{R} -linearly independent, their ratio does not lie on the real line. Interchanging ω_1, ω_2 if necessary, we may assume that $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Thus, we can use \mathcal{H} as a parameter space for all homothety classes of lattices, by identifying a point τ with the homothety class of the lattice $\tau \mathbb{Z} \oplus \mathbb{Z}$.
- Let $\Lambda_\tau = \tau \mathbb{Z} \oplus \mathbb{Z}$, and let $a\tau + b, c\tau + d$ be any basis for Λ_τ . Then:

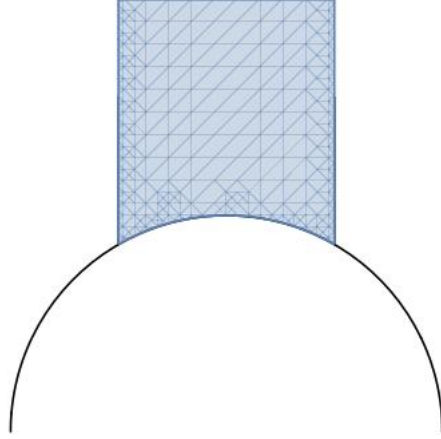
$$\Lambda_\tau = (a\tau + b)\mathbb{Z} \oplus (c\tau + d)\mathbb{Z} \sim \frac{1}{c\tau + d} ((a\tau + b)\mathbb{Z} \oplus (c\tau + d)\mathbb{Z}) = \frac{a\tau + b}{c\tau + d} \mathbb{Z} \oplus \mathbb{Z}$$

Thus, τ represents the same homothety class of lattices as $\frac{a\tau + b}{c\tau + d}$ for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$.

Thus, we only need to consider $SL_2(\mathbb{Z}) \backslash \mathcal{H}$ to classify homothety classes of lattices.

- Let $\tau \in \mathcal{H}$. Replacing τ by $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \tau = \tau + n$ if necessary, we can always find an element in the $SL(2, \mathbb{Z})$ orbit of τ satisfying $\frac{1}{2} < \Re(\tau) \leq \frac{1}{2}$. This amounts to replacing the generating set $\tau, 1$ with $\tau + n, 1$, which clearly does not change the lattice.
- Now, suppose $\tau \in \mathcal{H}$ and $|\tau| \leq 1$. Then $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \tau = \frac{-1}{\tau}$. At the level of lattices, this amounts to interchanging the two basis vectors and passing to the homothetic lattice where 1 is the shorter basis vector.
- Using the previous two operations, we can find a representative of each $SL_2(\mathbb{Z})$ -orbit in the domain:

$$\left\{ \tau \in \mathcal{H} : |\tau| \geq 1, \frac{-1}{2} < \Re(\tau) \leq \frac{1}{2} \right\}$$



1.1. **j -map.** We now have two descriptions of the moduli space of elliptic curves over \mathbb{C} :

- As \mathbb{C}^\times -orbits in $\mathcal{W}(\mathbb{C})$.
- As $SL_2(\mathbb{Z})$ -orbits of points in \mathcal{H} .

We give a final, much simpler description of the moduli space using the j -invariant.

The classical definition of the j -invariant is as a weight 0 modular form, i.e. $j : \mathcal{H} \rightarrow \mathbb{C}$ is a holomorphic function such that $j(\gamma \cdot \tau) = j(\tau)$ for all $\gamma \in SL_2(\mathbb{Z})$, and in fact j generates the algebra of holomorphic functions invariant under $SL_2(\mathbb{Z})$.

We can also define the j -invariant algebraically as the map:

$$j : \mathcal{W}(\mathbb{C}) \rightarrow \mathbb{C} \quad (f, g) \mapsto 1728 \frac{4f^3}{4f^3 + 27g^2}$$

Proposition 1.1. *Define a pair of elliptic curves:*

$$E : y^2 = x^3 + fx + g$$

$$E' : y^2 = x^3 + f'x + g'$$

The following are equivalent:

- (1) *There exists $t \in \mathbb{C}^\times$ such that $t^4 f = f'$ and $t^6 g = g'$.*
- (2) *E is isomorphic to E' as elliptic curves over \mathbb{C} .*
- (3) *The j -invariants of E, E' are equal.*

Proof. Assume (1). The map $E \rightarrow E'$ is $(x, y) \mapsto (t^2 x, t^3 y)$ is an isomorphism, so (1) implies (2). Furthermore:

$$j(E') = 1728 \frac{t^6(4f^3)}{t^6(4f^3 + 27g^2)} = 1728 \frac{4f^3}{4f^3 + 27g^2} = j(E)$$

so (1) implies (3).

Next, assume that $j(E) = j(E')$. If $j(E) \neq 0, 1728$, then f, g, f', g' are all nonzero. Let $u = \frac{fg'}{f'g}$ and $t = \sqrt{u}$.

Let t be a 4th root of $\frac{f'}{f}$. Then $t^4 f = f'$ by construction. We will show that $t^6 g = g'$.

$$\begin{aligned} 1728 \cdot 4f^3 = j(E)(4f^3 + 27g^2) &\implies t^{12} \cdot 17284f'^3 = t^{12} \cdot j(E)(4f^3 + 27g^2) \\ &\implies 17284f'^3 = j(E')(4f'^3 + 27(t^6g)^2) \\ &\implies (t^6g)^2 = g'^2 \end{aligned}$$

Thus $t^6 g = \pm g'$. Replacing t by it doesn't change t^4 , and negates t^6 in case $t^6 g = -g'$. Thus, if $j(E) = j(E')$, we can produce a $t \in \mathbb{C}$ such that $t^4 f = f', t^6 g = g'$. This proves (3) implies (1).

Finally, we show (2) implies (1). For this, it suffices to note that isomorphism between Weierstrass elliptic curves has to take x, y to scalar multiples of themselves, say $t_1 x, t_2 y$. The new equation is:

$$t_2^2 y^2 = t_1^3 x^3 + t_1 f x + g$$

We have to rescale this to put it in standard form:

$$y^2 = \frac{t_1^3}{t_2^2} + \frac{t_1}{t_2^2} f x + \frac{1}{t_2^2} g$$

We have no more freedom, but need the right hand side to be monic in for the new equation to also be in Weierstrass form. Thus, $t_1^3 = t_2^2$, i.e. t_1, t_2 must lie on the twisted cubic $u^3 = v^2$. Points on the twisted cubic are parametrized by $t \mapsto (t^2, t^3)$, so we can rewrite the map above as $x \mapsto t^2 x, y \mapsto t^3 y$. The relation satisfied by the new coefficients is:

$$(t^3 y)^2 = (t^2 x)^3 + (t^{-4} f)(t^2 x) + (t^{-6} g)$$

Thus, (2) implies (1). □

Altogether, we've shown that the map $j : \mathcal{W}(\mathbb{C})/\mathbb{C}^\times \rightarrow \mathbb{C}$ is a bijection, so our final description of the moduli space is simply as \mathbb{C} .

The final description will be helpful when we pass to non-algebraically closed fields. If k is a subfield of \mathbb{C} , then we can still parametrize elliptic curves over k using Weierstrass equations, i.e. we have a parameter space $\mathcal{W}(k)$ defined analogously to $\mathcal{W}(\mathbb{C})$.

The image of the composition $\mathcal{W}(k) \rightarrow \mathcal{W}(\mathbb{C})/\mathbb{C}^\times \rightarrow \mathbb{C}$ is exactly k : the j -invariant of any elliptic curve over k is clearly an element of k , and conversely, we can define an elliptic curve E/k with j -invariant j_0 for any $j_0 \in k$ using the construction above.

2. ELLIPTIC CURVES OVER \mathbb{R}

We would now like to give a description of the moduli space of elliptic curves over \mathbb{R} , up to isomorphism over \mathbb{R} .

2.1. $\mathcal{W}(\mathbb{R})/\mathbb{C}^\times$. We break the problem up into studying $\mathcal{W}(\mathbb{R})/\mathbb{C}^\times$, since it is a subset of a space we ostensibly understand, and then studying the fibers of $\mathcal{W}(\mathbb{R})/\mathbb{R}^\times \rightarrow \mathcal{W}(\mathbb{R})/\mathbb{C}^\times$.

To begin, we know that \mathbb{C} -isomorphism classes of elliptic curves over \mathbb{R} are in bijection with points on \mathbb{R} via the j -map. To understand the natural geometry of the moduli space better, it will be helpful to determine which points $\tau \in \mathcal{H}$ correspond to elliptic curves with real j -invariant. We know that $j(i) = 1728, j(e^{2\pi i/3}) = 0$, so we only need to find representatives for the intervals $(-\infty, 0), (0, 1728), (1728, \infty)$.

Let $\tau \in \mathcal{H}$ and assume $\Re(\tau) = 0$. An easy computation shows that $g_2(\tau), g_3(\tau) \in \mathbb{R}$, so points on the line $\Re(\tau) = 0$ represent elliptic curves with real j -invariants.

These elliptic curves have j -invariant in the range $(1728, \infty)$, and since they lie on the fundamental domain, they are all pairwise non-isomorphic (even over \mathbb{C}).

To find more examples of elliptic curves with $g_2, g_3 \in \mathbb{R}$. We may need to rotate the lattices to obtain representatives in the homothety class with $g_2(\Lambda), g_3(\Lambda)$, so we start by proving a general lemma that does not assume we're working with a lattice of the form $\tau\mathbb{Z} \oplus \mathbb{Z}$.

Let $\tau \in \mathcal{H}$ and assume that $\tau, \bar{\tau}$ are \mathbb{R} -linearly independent (so basically $\tau \neq it$ for $t \in \mathbb{R}$). Let $\Lambda = \tau\mathbb{Z} \oplus \bar{\tau}\mathbb{Z}$. Then $g_k(\Lambda) \in \mathbb{R}$ for all k .

To see this, we note that:

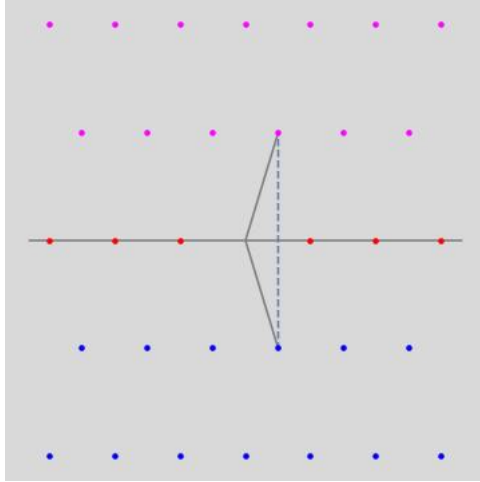
$$g_k(\Lambda) = \sum \lambda^{2k}$$

where the sum is taken over all nonzero elements of the lattice.

We split Λ' into three sets:

- Points $m\tau + n\bar{\tau}$ with $m > n$.
- Points of the form $m\tau + n\bar{\tau}$ with $m = n$.
- Points of the form $m\tau + n\bar{\tau}$ with $m < n$.

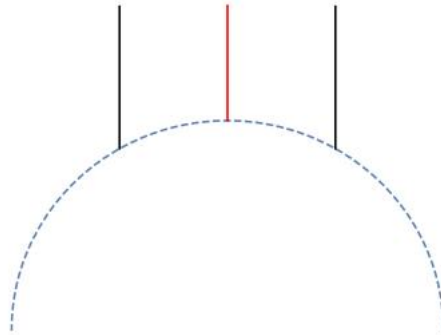
Note that complex conjugation acts on the lattice, interchanging points with $m > n$ and points with $m < n$ while fixing points with $m = n$ pointwise.



Thus, $g_k(\Lambda)$ can be broken up into three subseries, one of which is guaranteed to be real, and the other two complex conjugates of each other. Thus $g_k(\Lambda)$ is real, since the sum of complex conjugates is always real.

In particular, if $\Re(\tau) = \frac{1}{2}$, then the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$ gives rise to a real elliptic curve, since we can take $\tau, 1 - \tau$ as a generating set for the lattice, and $\overline{1 - \tau} = \bar{\tau}$.

Thus, the following rays on the usual fundamental domain represent elliptic curves with real j -invariant:



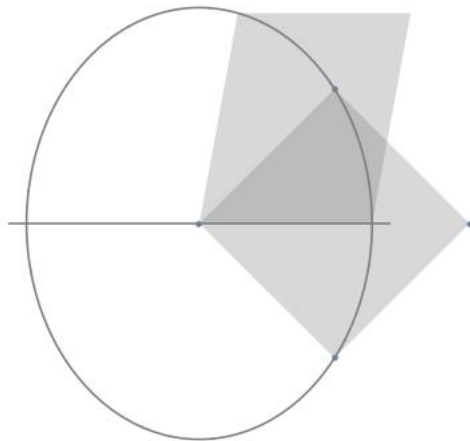
The red line represents elliptic curves with $j \geq 1728$ and the black lines represent elliptic curves with $j \leq 0$. We still need to find representatives for the elliptic curves with j -invariant in the range $(0, 1728)$, but no other points in the usual fundamental domain have $g_2, g_3 \in \mathbb{R}$.

To check that $j(\tau) \in \mathbb{R}$, it is equivalent to show $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$ for Λ a lattice homothetic to $\tau\mathbb{Z} \oplus \mathbb{Z}$.

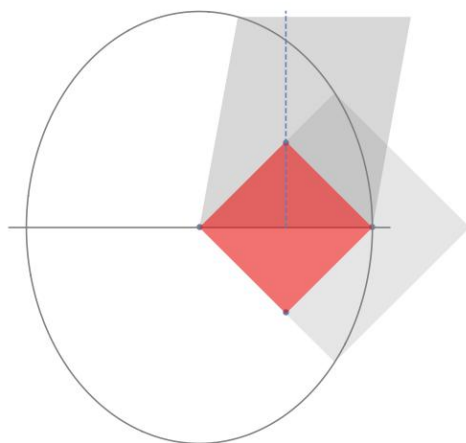
Let $\tau = e^{i\theta}$. We can rotate the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$ so that the generators are equidistant from the real line. Precisely, if $\rho = \sqrt{\tau}$, then:

$$\rho^{-1} \cdot (\tau\mathbb{Z} \oplus \mathbb{Z}) = \rho\mathbb{Z} \oplus \rho^{-1}\mathbb{Z} = \rho\mathbb{Z} \oplus \bar{\rho}\mathbb{Z}$$

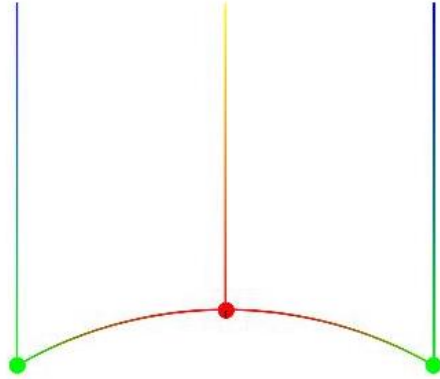
where the final equality follows from the fact that $\frac{1}{\rho} = \bar{\rho}$ for ρ on the unit circle. This new lattice has the same j -invariant as the original and has a real j -invariant.



Note that this new lattice is \mathbb{R} -isomorphic to a lattice represented by a point $\tau \in \mathcal{H}$; we simply rescale the lattice by a real number so that $\tau + \bar{\tau} = 1$. The rescaled lattice can then be generated by $1, \frac{\tau}{\tau + \bar{\tau}}$. Further note that the real part of $\frac{\tau}{\tau + \bar{\tau}}$ is always exactly $\frac{1}{2}$.



In any case, this shows that $j(e^{i\theta}) \in \mathbb{R}$, and as θ varies between $\frac{\pi}{3}, \frac{\pi}{2}$, the j -invariant goes from 0 to 1728. Thus, we can complete our picture of \mathbb{C} -isomorphism classes of real elliptic curves:



2.2. Quadratic Twisting. The next step is understanding the fibers of $\mathcal{W}(\mathbb{R})/\mathbb{R}^\times \rightarrow \mathcal{W}(\mathbb{R})/\mathbb{C}^\times$. If we have two elements $(f, g), (f', g') \in \mathcal{W}(\mathbb{R})$ that map to the same element in $\mathcal{W}(\mathbb{R})/\mathbb{C}^\times$, then there exists $t \in \mathbb{C}^\times$ such that $t \cdot (f, g) = (f', g')$. Since $f, f' \in \mathbb{R}$, this means $t^4 \in \mathbb{R}$ and since $g, g' \in \mathbb{R}$, we must have $t^6 \in \mathbb{R}$. Combining these two observations, we must have $t^2 \in \mathbb{R}$, so either $t \in \mathbb{R}^\times$ or $it \in \mathbb{R}^\times$. If $t \in \mathbb{R}^\times$, then $[(f, g)] = [(f', g')]$ in $\mathcal{W}(\mathbb{R})/\mathbb{R}^\times$. Thus each \mathbb{C} -isomorphism class of elliptic curves over \mathbb{R} splits up into two \mathbb{R} -isomorphism classes of real elliptic curves, i.e. $\mathcal{W}(\mathbb{R})/\mathbb{R}^\times \rightarrow \mathcal{W}(\mathbb{R})/\mathbb{C}^\times$ is a double cover.

Two elliptic curves $E, E'/\mathbb{R}$ are quadratic twists of each other if they are not isomorphic over \mathbb{R} , but become isomorphic over \mathbb{C} . For a given elliptic curve:

$$E : y^2 = x^3 + fx + g \quad (f, g \in \mathbb{R})$$

we can obtain an equation for the quadratic twist by replacing y by iy and x by $-x$ (and multiplying the equation by -1):

$$E' : y^2 = x^3 + fx - g$$

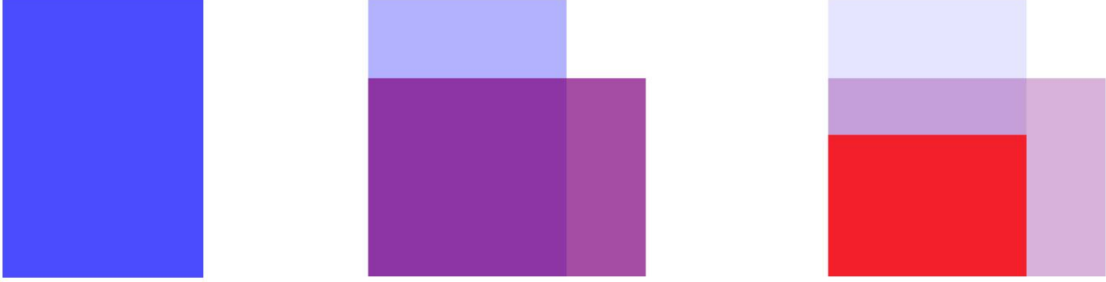
If $g = 0$, then $E = E'$, but the following elliptic curve:

$$E'' : y^2 = x^3 - fx$$

is a quadratic twist of E .

Note that this corresponds, at the level of lattices, to replacing Λ by $i\Lambda$, since $g_2(i\Lambda) = g_2(\Lambda)$ and $g_3(i\Lambda) = -ig_3(\Lambda)$. For example, if $\Lambda = s\mathbb{Z} \oplus \mathbb{Z}$ for some $s > 1$, then $i\Lambda = i\mathbb{Z} \oplus s\mathbb{Z} =$

$s(\frac{i}{s}\mathbb{Z} \oplus \mathbb{Z})$. Thus, $si, \frac{1}{s}i \in \mathcal{H}$ represent elliptic curves which are isomorphic over \mathbb{C} , but not iso-



morphic over \mathbb{R} .

Thus, if we extend the original fundamental domain to contain all $\tau \in \mathcal{H}$ with $\Re(\tau) = 0$, then we have exactly one representative for each \mathbb{R} -isomorphism class of elliptic curve with $j > 1728$. The elliptic curve with $j = 1728$ only has one representative on this line, since $\frac{1}{\Im\tau} = \Im(\tau)$.

2.3. $\Re(\tau) = \frac{1}{2}$. We can do something similar with τ on the line $\Re(\tau) = \frac{1}{2}$.

Let $\tau = \frac{1}{2} + it$ for $t \in \mathbb{R}^+$. Recall that $\tau\mathbb{Z} \oplus \mathbb{Z} = \tau\mathbb{Z} \oplus \bar{\tau}\mathbb{Z}$, so:

$$i(\tau\mathbb{Z} \oplus \mathbb{Z}) = i\tau\mathbb{Z} \oplus i\bar{\tau}\mathbb{Z} = i\tau\mathbb{Z} \oplus -i\bar{\tau}\mathbb{Z} = i\tau\mathbb{Z} \oplus \overline{i\tau}\mathbb{Z}$$

We rescale this as in () to obtain a new generating set $\tau' = \frac{i\tau}{2\Re(i\tau)}, 1$. Now, compute:

$$\Re(\tau') = \frac{\Re(i\tau)}{2\Re(i\tau)} = \frac{1}{2} \quad \Im(\tau') = \frac{\Im(i\tau)}{2\Re(i\tau)} = \frac{\frac{1}{2}}{-2t} = \frac{1}{-4t}$$

Thus $\tau' = \frac{1}{2} + i\frac{1}{-4t}$. Since $1, 1 - \tau' = \frac{1}{2} + i\frac{1}{4t}$ is also a generating set, we see that quadratic twisting acts on the line $\Re(\tau) = \frac{1}{2}$ by $\tau \mapsto \frac{1}{2} + \frac{i}{4\Im(\tau)}$. Note that this involution has a unique fixed point at $\tau = \frac{1+i}{2}$, which represents the elliptic curve with $j = 1728$.

Thus, points with negative j -invariant are represented by τ with $\Re(\tau) = \frac{1}{2}$ and either $\Im(\tau) \geq \frac{\sqrt{3}}{2}$ or $\Im(\tau) \leq \frac{1}{2\sqrt{3}}$. Furthermore, we saw earlier that points on the unit circle represent lattices which are homothetic to lattices represented by point on the line $\Re(\tau) = \frac{1}{2}$, so we can find representatives for elliptic curves with j -invariant in $(0, 1728)$ on the same line.

This completes the picture of the moduli space:

- Every $j > 1728$ has two non-isomorphic representatives on the line $\Re(\tau) = 0$, and $j = 1728$ has exactly one representative on that line.
- Every $j < 1728$ has two representatives on the line $\Re(\tau) = \frac{1}{2}$, one with $\Im(\tau) > \frac{1}{2}$ and one with $\Im(\tau) < \frac{1}{2}$. The two representatives are nontrivial quadratic twists of

each other. We also have a single representative for the elliptic curve with $j = 1728$, which represents the quadratic twist of $\tau = i$.

Thus, the two lines $\Re(\tau) = 0$ and $\Re(\tau) = \frac{1}{2}$ contain exactly one representative for each \mathbb{R} -isomorphism class of elliptic curves. We also have additional representatives for these points on the fundamental domain.

The following picture therefore depicts the moduli space of elliptic curves over \mathbb{R} :

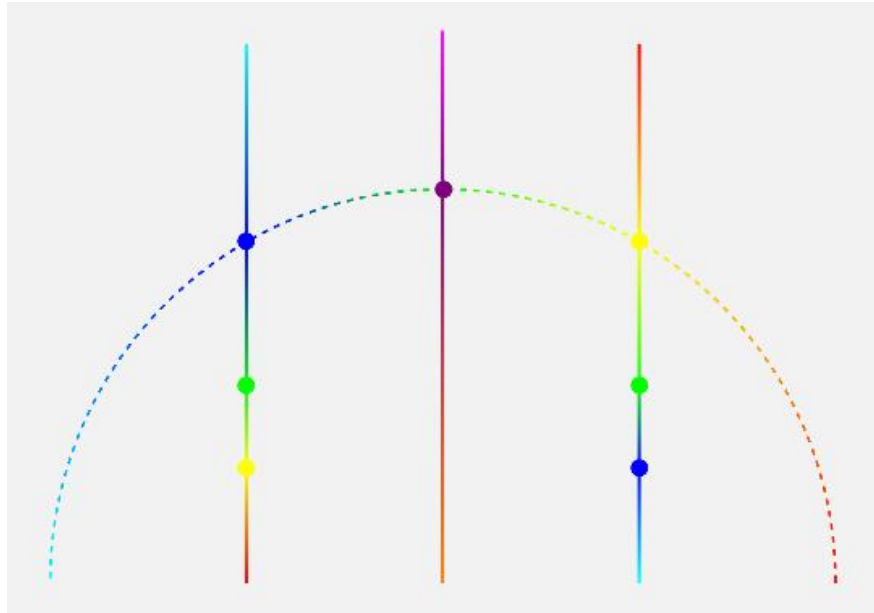


FIGURE 1. The moduli space of real elliptic curves up to real isomorphism. Color is used to distinguish between \mathbb{R} -isomorphism classes.