THE MODULAR CURVES $X_0(11)$ AND $X_1(11)$

TOM WESTON

This paper is intended as a brief introduction to the theory of moduli spaces through the concrete examples of certain modular curves. The motivating question, which we seek to answer, is whether or not there exist any rational elliptic curves over $\mathbb{Q}$ with a rational point of order 11. This problem, which seems quite hopeless in terms of explicit polynomials, turns out to have a beautiful solution in terms of modular curves.

The portions of this paper dealing with explicit computations for $X_0(11)$ are based on a talk given by Matthew Emerton, incorporating some modifications by Keith Conrad and Robert Pollack. Throughout the paper all algebraic curves are assumed to be smooth and projective. We give very few complete proofs; to give complete details would have made the paper many times longer, and we will be content to give the main ideas.

1. The j-line

For this section we are interested in classifying elliptic curves up to isomorphism; if K is a field, we will denote by $\mathrm{Ell}(K)$ the set of isomorphism classes of elliptic curves defined over K. Here we consider two elliptic curves E_1 and E_2 over K to be isomorphic if there is an isomorphism $E_1 \to E_2$ defined over K.

We will begin with a description of $\mathrm{Ell}(\mathbb{C})$. Recall that an elliptic curve over $\mathbb{C}$ can be realized as $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$; here by lattice we mean a free $\mathbb{Z}$-module of rank 2 generated by two $\mathbb{R}$-linearly independent complex numbers. If ω_1, ω_2 are complex numbers which are linearly independent over $\mathbb{R}$, we will write $\langle \omega_1, \omega_2 \rangle$ for the lattice which they generate. Two complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic (over $\mathbb{C}$) if and only if the lattices Λ_1 and Λ_2 are *homothetic*; that is, if there is some $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$. (To go from the $\mathbb{C}/\Lambda$ form to the usual Weierstrass form $y^2 = x^3 + ax + b$ one uses the Weierstrass functions and its derivative; for details on all of this, see [14, Chapter 6] and [15, Chapter 1].)

Using this description of complex elliptic curves, we see that in order to get a description of $\mathrm{Ell}(\mathbb{C})$ it will suffice for us to classify lattices up to homothety. We summarize the construction; see [13, Chapter 7, Sections 1 and 2] or [15, Chapter 1, Sections 1 and 2] for more details. The first step is to normalize the lattices somewhat. Whenever we are dealing with a basis $\langle \omega_1, \omega_2 \rangle$ of a lattice Λ, we will assume that ω_1, ω_2 are ordered so that $\mathrm{Im}\, \omega_2/\omega_1 > 0$. This lattice Λ is homothetic to the lattice $\Lambda_\tau = \langle 1, \tau \rangle$, where $\tau = \omega_2/\omega_1$; thus we can restrict our attention to lattices of this form Λ_τ with $\tau \in \mathcal{H}$, $\mathcal{H}$ denoting the upper half plane in $\mathbb{C}$.

Two such lattices can still be homothetic. To determine when this happens, we consider a single lattice Λ_τ. The possible ordered bases of Λ_τ are precisely the bases $\langle c\tau + d, a\tau + b \rangle$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. (Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 matrices with integer entries and determinant 1. Here the positive determinant condition insures that our basis will still satisfy $\frac{a\tau+b}{c\tau+d} \in \mathcal{H}$.) These lattices are in turn homothetic to the lattices $\Lambda_{\tau'}$ with $\tau' = \frac{a\tau+b}{c\tau+d}$, and these are the only lattices of this form which are homothetic to Λ_τ.

We rephrase our results as follows: we define an action of the group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

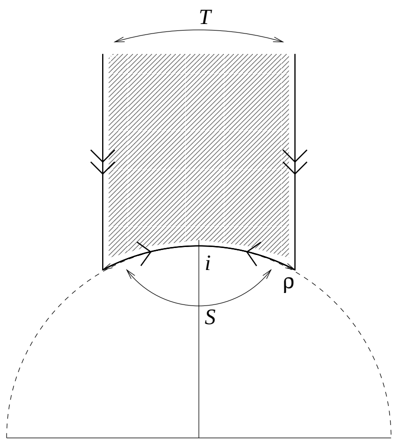
(One checks easily that this really is a group action.) We have a map from $\mathcal{H}$ to the set of homothety classes of lattices given by $\tau \mapsto \Lambda_\tau$, and two lattices Λ_τ and $\Lambda_{\tau'}$ are homothetic if and only if there is some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma\tau = \tau'$. That is, we can regard isomorphism classes of lattices as parametrized by the orbit space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. (We write the group in this quotient on the left since it acts on $\mathcal{H}$ on the left.) This in turn allows us to identify isomorphism classes of complex elliptic curves with elements of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$:

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} &\longleftrightarrow \mathrm{Ell}(\mathbb{C}) \\ \tau &\longrightarrow \mathbb{C}/\Lambda_\tau \\ \frac{\omega_2}{\omega_1} &\longleftarrow \mathbb{C}/\langle \omega_1, \omega_2 \rangle \end{aligned}$$

One can show (see [13, Chapter 7, Theorem 2] or [15, Chapter 1, Corollary 1.6]) that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices

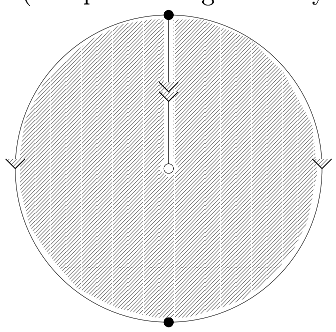
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

these act on $\mathcal{H}$ by $S(\tau) = -1/\tau$ and $T(\tau) = \tau + 1$. It follows easily (see [13, Chapter 7, Theorem 1] or [15, Chapter 1, Proposition 1.5]; in fact, one usually proves the last two facts simultaneously) that a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ is given by the following region: (For this region to be a fundamental domain just means that every $\mathrm{SL}_2(\mathbb{Z})$-orbit on $\mathcal{H}$ corresponds to a unique point of the region.)



The arrows on the boundary lines indicate that these lines are identified by the given transformations. ρ is the sixth root of unity $\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Note that on identifying the edges of this region one appears to obtain a sphere with a single point removed (this point being infinitely far up the imaginary axis).



On inserting this point (which is called the *cusp at infinity* and written as $i\infty$) one obtains (at least topologically) a sphere. In fact, it is possible to define a complex structure on this space (this is the obvious complex structure at most points, although one has to be a little careful at ρ, i and the cusp $i\infty$), making it into a compact *Riemann surface*; see [14, Chapter 1, Section 2]. (A Riemann surface is essentially just a topological space for which every point has a neighborhood isomorphic to an open subset of $\mathbb{C}$.) When regarding it from this point of view, we will denote this Riemann surface by $X(1)$; denoting by $\mathcal{C}$ the set containing the cusp, we have

$$X(1) = (\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}) \cup \mathcal{C}.$$

Our description above shows that it is isomorphic the the *Riemann sphere* $\mathbb{P}^1(\mathbb{C})$.

The Riemann sphere is usually obtained by adding a single point at infinity to the complex plane $\mathbb{C}$. From this point of view it is easy to determine the meromorphic functions on $\mathbb{P}^1(\mathbb{C})$: let $f(z)$ be such a function, which we regard as a function on $\mathbb{C}$. Since $f(z)$ does not have an essential singularity at infinity, it only has poles in some bounded region of $\mathbb{C}$ and therefore has finitely many poles. We can multiply $f(z)$ by polynomials to eliminate these poles, and we are left with a function $g(z)$ which has a pole at infinity and no other poles. Suppose that this pole has order n. The standard function with an order n pole at ∞ is z^n, which is holomorphic on the rest of $\mathbb{P}^1(\mathbb{C})$. So subtract from $g(z)$ an appropriate multiple of z^n to obtain a function $h(z)$ with a pole at infinity of order at most $n-1$ and no other poles. Continuing in this way we find that we can subtract a polynomial from $g(z)$ to obtain a function which has no poles on $\mathbb{C}$ or at infinity; by Liouville's theorem such a function is a constant. Thus $g(z)$ is a polynomial, and $f(z)$ is rational function. We conclude that the field of meromorphic functions on $\mathbb{P}^1(\mathbb{C})$ is just the field $\mathbb{C}(z)$ of rational functions in z. (The fundamental reason why there are so few meromorphic functions on $\mathbb{P}^1(\mathbb{C})$ is that it, unlike $\mathbb{C}$, is compact.)

We conclude that the function field of $X(1)$ is generated over $\mathbb{C}$ by a single transcendental function. Regarding points of $X(1)$ as isomorphism classes of elliptic curves $\mathbb{C}/\Lambda$, the standard choice of such a function is the function j which sends an elliptic curve to its j-invariant, which is a complex number which classifies it up to isomorphism. (See [14, Chapter 3, Section 1].) Regarding j as a function of the coordinate τ on $\mathcal{H}$, we have the identity

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, since $\frac{a\tau+b}{c\tau+d}$ and τ give rise to the same point of $X(1)$. This means that j is a *modular form of weight* 0, otherwise known as a modular function. In particular, $j(\tau+1) = j(\tau)$, so we can write out a Fourier expansion for j in terms of $q = e^{2\pi i\tau}$. It can be shown that

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots;$$

see [15, Chapter 1, Remark 7.4].

Recall that the algebraic curve $\mathbb{P}^1_{\mathbb{C}}$ also has a function field $\mathbb{C}(z)$. This suggests that we should be able to regard the Riemann sphere as an algebraic curve. In fact, both complex algebraic curves and compact Riemann surfaces are uniquely determined by their function fields, which are finitely generated field extensions of $\mathbb{C}$ of transcendence degree 1. This sets up a bijection between complex algebraic curves and Riemann surfaces: we associate to the (unique) complex algebraic curve X with function field K the (unique) Riemann surface X' with function field K. This bijection turns out to respect all of the other relevant structure as well; in particular, X and X' have the same sets of points: $X(\mathbb{C}) = X'(\mathbb{C})$.

In summary, we have seen that the set of isomorphism classes of complex elliptic curves is in natural bijection with the non-cuspidal points of a complex algebraic curve $X(1)_{\mathbb{C}}$:

$$X(1)_{\mathbb{C}}(\mathbb{C}) \longleftrightarrow \mathrm{Ell}(\mathbb{C}) \cup \mathcal{C}.$$

We have also seen that $X(1)_{\mathbb{C}}$ is isomorphic to the projective line $\mathbb{P}^1_{\mathbb{C}}$.

Of course, the curve $\mathbb{P}^1_{\mathbb{C}}$ can actually be defined over $\mathbb{Q}$ as the projective line $\mathbb{P}^1_{\mathbb{Q}}$ with function field $\mathbb{Q}(j)$; the fact that $\mathbb{C}\mathbb{Q}(j) = \mathbb{C}(j)$ means that $\mathbb{P}^1_{\mathbb{Q}}(\mathbb{C}) = \mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$. Thus, setting $X(1)_{\mathbb{Q}} = \mathbb{P}^1_{\mathbb{Q}}$, we have a bijection

$$X(1)_{\mathbb{Q}}(\mathbb{C}) \longleftrightarrow \mathrm{Ell}(\mathbb{C}) \cup \mathcal{C}.$$

Since we have defined $X(1)_{\mathbb{Q}}$ over $\mathbb{Q}$, one might hope that we also obtain a bijection between the $\mathbb{Q}$-valued points of $X(1)_{\mathbb{Q}}$ and isomorphism classes of elliptic curves over $\mathbb{Q}$. Unfortunately, this is not the case: there is a map

$$\mathrm{Ell}(\mathbb{Q}) \to \mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$$

sending an elliptic curve to its j-invariant, but it is not a bijection. This is because if two elliptic curves over $\mathbb{Q}$ have the same j-invariant it does not mean that there exists an isomorphism between them defined over $\mathbb{Q}$, but only that such an isomorphism exists over $\bar{\mathbb{Q}}$. Thus the non-cuspidal points $X(1)_{\mathbb{Q}}(\mathbb{Q})$ classify elliptic curves over $\mathbb{Q}$ only up to isomorphism over $\bar{\mathbb{Q}}$.

2. Modular pairs

We now seek to redo the construction of the previous section for a slightly different class of objects. We define a *modular pair* over a field K to be a pair (E, C) of an elliptic curve over K and a cyclic subgroup C of $E(\bar{K})$ of order 11. We further require that every σ in the Galois group $\mathrm{Gal}(\bar{K}/K)$ maps C to itself. This is certainly the case if C actually lies in $E(K)$, but this is not necessary; essentially all that we are requiring is that each σ sends each element of C to a multiple of itself. Two modular pairs (E_1, C_1) and (E_2, C_2) over K will be considered to be isomorphic if there is an isomorphism of E_1 with E_2, defined over K, which sends C_1 to C_2.

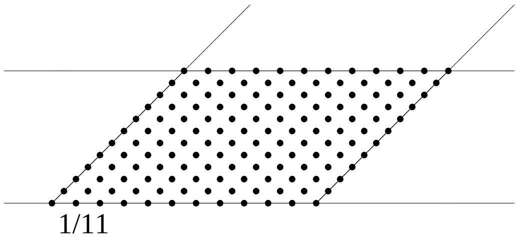


FIGURE 1. The 11-torsion on a complex elliptic curve

We begin as before with the situation over the complex numbers. Here we can consider modular pairs as pairs $(\mathbb{C}/\Lambda, C)$, and two pairs $(\mathbb{C}/\Lambda_1, C_1)$ and $(\mathbb{C}/\Lambda_2, C_2)$ are isomorphic if there exits a complex number α such that $\alpha\Lambda_1 = \Lambda_2$ and $\alpha C_1 \equiv C_2 \pmod{\Lambda_2}$.

If $(\mathbb{C}/\Lambda, C)$ is a modular pair, we can regard $C + \Lambda$ as a complex lattice in its own right; we have $\Lambda \subseteq C + \Lambda$, and the condition that C has order 11 means precisely that $(C + \Lambda)/\Lambda$ has order 11. We can therefore think of modular pairs as pairs $\Lambda_1 \subseteq \Lambda_2$ of complex lattices such that Λ_2/Λ_1 has order 11; the associated modular pair is $(\mathbb{C}/\Lambda_1, \Lambda_2/\Lambda_1)$. By the structure theorem for finitely generated abelian groups we can find a basis $\langle \omega_1, \omega_2 \rangle$ of Λ_1 such that $\left\langle \frac{1}{11}\omega_1, \omega_2 \right\rangle$ is a basis for Λ_2; as usual we can also assume that ω_2/ω_1 has positive imaginary part. This modular pair is isomorphic to the modular pair $(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\mathbb{Z})$ (corresponding to the inclusion of lattices $\Lambda_\tau \subseteq \frac{1}{11}\mathbb{Z} + \Lambda_\tau$) with $\tau = \omega_2/\omega_1 \in \mathcal{H}$; the isomorphism is given by the homothety $\omega_1^{-1} : C/\Lambda_1 \to \mathbb{C}/\Lambda_\tau$.

Combining all of this, we can associate to every modular pair $(\mathbb{C}/\Lambda, C)$ a complex number $\tau \in \mathcal{H}$ such that $(\mathbb{C}/\Lambda, C)$ is isomorphic to the $(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\mathbb{Z})$. The difference between this and the situation of the previous section is that $\tau_1, \tau_2 \in \mathcal{H}$ give rise to isomorphic modular pairs if and only if $(\mathbb{C}/\Lambda_{\tau_1}, \frac{1}{11}\mathbb{Z}) \cong (\mathbb{C}/\Lambda_{\tau_2}, \frac{1}{11}\mathbb{Z})$ as modular pairs.

To sort out this condition, we proceed as in the previous section and fix one τ. The possible bases for Λ_τ are those of the form $\langle c\tau + d, a\tau + b \rangle$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. These in turn are associated to lattices $\Lambda_{\tau'}$ with $\tau' = \frac{a\tau+b}{c\tau+d}$. However, not all such τ' correspond to τ when the extra structure of the cyclic subgroup of order 11 is taken into account.

We must determine for which $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ the modular pair $(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\mathbb{Z})$ is isomorphic to the modular pair $(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{11}\mathbb{Z})$. The homothety of Λ_τ and $\Lambda_{\tau'}$ is given by multiplication by $c\tau + d$; this homothety takes $\frac{1}{11}\mathbb{Z}$ to $\frac{1}{11}\mathbb{Z}$ if and only if

$$(c\tau + d)\frac{1}{11}\mathbb{Z} \equiv \frac{1}{11}\mathbb{Z} \pmod{\Lambda_\tau}.$$

Since d is an integer and 1 and τ are linearly independent this is the same as requiring that $\frac{c\tau}{11}$ is a multiple of τ. Of course, this is the case if and only if 11 divides c. We conclude that a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ takes $(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\mathbb{Z})$ to $(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{11}\mathbb{Z})$ if and only if 11 divides c.

Define $\Gamma_0(11) \subseteq \mathrm{SL}_2(\mathbb{Z})$ to be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of such matrices:

$$\Gamma_0(11) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{11}\}.$$

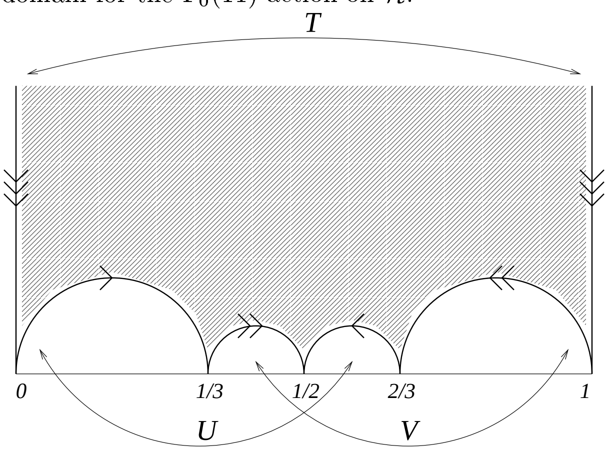
Our arguments to this point have shown that we can identify modular pairs over $\mathbb{C}$ with points of $\mathcal{H}$ modulo the action of $\Gamma_0(11)$; that is, we can identify them with the orbit space $\Gamma_0(11)\backslash\mathcal{H}$:

$$\begin{aligned} \Gamma_0(11)\backslash\mathcal{H} &\longleftrightarrow \mathrm{Ell}_0(\mathbb{C}) \\ \tau &\longrightarrow \left(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\mathbb{Z}\right) \end{aligned}$$

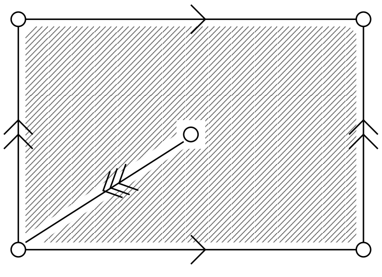
We would like a description of $\Gamma_0(11)\backslash\mathcal{H}$ as a Riemann surface. To do this we will need a fundamental domain. It can be shown that the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad U = \begin{pmatrix} 7 & -2 \\ 11 & -3 \end{pmatrix} \qquad V = \begin{pmatrix} 8 & -3 \\ 11 & -4 \end{pmatrix}$$

generate $\Gamma_0(11)$. Using this and a little care one can show that the region below is a fundamental domain for the $\Gamma_0(11)$-action on $\mathcal{H}$.



When one identifies the lines $\tau = 0$ and $\tau = 1$, the region can be drawn in the following simpler way:



We see now that $\mathcal{H}\backslash\Gamma_0(11)$ is almost a torus, except that it is missing two points. We call the missing interior point the *cusp at infinity* and the missing corner point the *cusp at zero*, and we let $\mathcal{C}_0$ denote the set of these two points. Once these points are added, $\Gamma_0(11)\backslash\mathcal{H}$ is a torus. In fact, as with $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, it is possible to give $\Gamma_0(11)\backslash\mathcal{H}$ the structure of a Riemann surface which we denote $X_0(11)$; see [7, Chapter 11, Section 2]. From our construction, we have a bijection

$$X_0(11) \longleftrightarrow \mathrm{Ell}_0(\mathbb{C}) \cup \mathbb{C}.$$

It is important to note that we add the cusps only so that $X_0(11)$ becomes compact; they do not correspond to honest elliptic curves. In particular, after we have defined $X_0(11)$ as an algebraic curve over $\mathbb{Q}$, the cusps will yield two rational points which don't actually correspond to elliptic curves.

3. $X_0(11)$ as an elliptic curve over $\mathbb{Q}$

The first key to using $X_0(11)$ to analyze elliptic curves over $\mathbb{Q}$ is to show that it can actually be realized as a curve defined over $\mathbb{Q}$. As it is, we have $X_0(11)$ as a Riemann surface. As we have said before, every Riemann surface corresponds to a complex algebraic curve, so we can also regard $X_0(11)$ in this way; when we do so we will write it as $X_0(11)_\mathbb{C}$. Let L be its function field; it is a finitely generated extension of $\mathbb{C}$ of transcendence degree 1.

To show that $X_0(11)_\mathbb{C}$ can actually be defined over $\mathbb{Q}$, we must find a finitely generated field extension K of $\mathbb{Q}$ of transcendence degree 1 such that $\mathbb{C}K = L$. Indeed, we can then define $X_0(11)_\mathbb{Q}$ to be the algebraic curve corresponding to K; the fact that $\mathbb{C}K = L$ will insure that $X_0(11)_\mathbb{Q}(\mathbb{C})$ recovers our previous complex algebraic curve $X_0(11)_\mathbb{C}$.

There are several approaches to defining the field K. The first approach begins by explicitly determining L as the field of meromorphic functions on $X_0(11)$ regarded as a Riemann surface. To do this, we must exhibit some rational functions on $X_0(11)$. The first is the function j we had on $X(1)$; it still makes sense as a function on $X_0(11)$ since $\Gamma_0(11) \subseteq \mathrm{SL}_2(\mathbb{Z})$.

Let $j_{11}(\tau) = j(11\tau)$. We claim that j_{11} is also a function on $X_0(11)$. To show this, we must check that

$$j_{11}\left(\frac{a\tau + b}{c\tau + d}\right) = j_{11}(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$, for then j_{11} descends from a function on $\mathcal{H}$ to a function on $\Gamma_0(11)\backslash\mathcal{H} = X_0(11)$. We compute

$$\begin{aligned} j_{11}\left(\frac{a\tau + b}{c\tau + d}\right) &= j\left(11\frac{a\tau + b}{c\tau + d}\right) \\ &= j\left(\frac{a(11\tau) + 11b}{\frac{c}{11}(11\tau) + d}\right) \\ &= j(11\tau) \\ &= j_{11}(\tau) \end{aligned}$$

since $\begin{pmatrix} a & 11b \\ c/11 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and j is $\mathrm{SL}_2(\mathbb{Z})$-invariant.

We have now exhibited two meromorphic functions on $X_0(11)$. One can show that $L = \mathbb{C}(j, j_{11})$; that j_{11} is a root of a polynomial $\Phi(x)$ in $\mathbb{Z}[j, x]$; and that $\Phi(x)$ is irreducible as a polynomial over $\mathbb{C}(j)$. See [7, Chapter 11, Section 6].

One can use the above assertions to realize $X_0(11)_\mathbb{C}$ as an algebraic curve over $\mathbb{Q}$. Indeed, we simply define $K = \mathbb{Q}(j)[j_{11}]/\Phi(j_{11})$, where we are regarding j as an abstract transcendental element and j_{11} as a formal variable; let $X_0(11)_\mathbb{Q}$ be the associated algebraic curve over $\mathbb{Q}$. This makes sense, since $\Phi(x)$ has coefficients in $\mathbb{Z}[j]$. The fact that $\Phi(x)$ is irreducible over $\mathbb{C}(j)$ insures us that $\mathbb{C}K$ really is just $L = \mathbb{C}(j)[j_{11}]/\Phi(j_{11})$.

There is a second approach to defining $X_0(11)_{\mathbb{Q}}$. This approach does not use the Riemann surface description of $X_0(11)$ at all. We only sketch the main ideas; see [12, Section 1] for details. We begin with the elliptic curve E

$$y^2 = 4x^3 - \frac{27t}{t-1728}x - \frac{27t}{t-1728}$$

defined over the field $\mathbb{Q}(t)$. This curve has the property that its j-invariant is just t. Let $\mathbb{Q}(t, E[11])$ be the extension of $\mathbb{Q}(t)$ generated by the coordinates of the points of E of order 11. Fixing a basis P, Q of $E[11]$, we can regard $E[11]$ as a two dimensional vector space over $\mathbb{Z}/11\mathbb{Z}$. $\mathrm{Gal}(\mathbb{Q}(t, E[11])/\mathbb{Q})$ acts on $E[11]$ in a natural way, and we therefore obtain a map

$$\mathrm{Gal}(\mathbb{Q}(t, E[11])/\mathbb{Q}) \to \mathrm{Aut}(E[11]) \cong \mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z}),$$

(the isomorphism coming from our fixed basis P, Q) which one easily sees is injective. It is a much deeper fact that it is actually an isomorphism.

Let H be the subgroup of $GL_2(\mathbb{Z})$ which maps the cyclic subgroup generated by Q to itself; one finds that

$$H = \left\{ \begin{pmatrix} a & 0 \\ b & d \end{pmatrix} \mid a, d \in (\mathbb{Z}/11\mathbb{Z})^*, b \in \mathbb{Z}/11\mathbb{Z} \right\}.$$

This corresponds to a subgroup of $\mathrm{Gal}(\mathbb{Q}(t, E[11])/\mathbb{Q}(t))$ by our above isomorphism, and we let K be the fixed field of $\mathbb{Q}(t, E[11])$ by this subgroup. One defines $X_0(11)_{\mathbb{Q}}$ to be the algebraic curve over $\mathbb{Q}$ corresponding to K. Of course, one now has to show that K really is the same as the field we constructed before; this amounts to getting a better understanding of the polynomial $\Phi(x)$.

Using either of the two methods, we have shown that the Riemann surface $X_0(11)$ can be represented by an algebraic curve $X_0(11)_{\mathbb{Q}}$ over $\mathbb{Q}$. Recall that we found that the Riemann surface $X_0(11)$ is a torus; that is, it has genus 1. Since the complex points on $X_0(11)_{\mathbb{Q}}$ yield a space of genus 1, it follows that $X_0(11)_{\mathbb{Q}}$ itself is an elliptic curve. $X_0(11)_{\mathbb{Q}}$ therefore has a Weierstrass equation; we will determine what it is in the next section.

Now that we have realized $X_0(11)_{\mathbb{Q}}$ as a curve over $\mathbb{Q}$, we can ask if our description of the points on this curve has the same interpretation it had over $\mathbb{C}$. That is, we can ask if the points $X_0(11)_{\mathbb{Q}}(\mathbb{Q})$ correspond to pairs (E, C) of elliptic curves over $\mathbb{Q}$ and cyclic subgroups of order 11 stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, up to isomorphism over $\mathbb{Q}$. Unfortunately, this does not quite work out; there is a natural map

$$\{\text{modular pairs } (E, C) \text{ over } \mathbb{Q} \text{ up to isomorphism}\} \to X_0(11)_{\mathbb{Q}}(\mathbb{Q}) - \mathcal{C}_0$$

but it is a priori not necessarily a surjection or an injection. We will have more to say about these rational points later.

4. An equation for $X_0(11)$

Since $X_0(11)_{\mathbb{Q}}$ is an elliptic curve defined over $\mathbb{Q}$ we can hope to find an equation for it. This turns out to be a fairly involved exercise in modular functions. One could attempt to carry out these calculations with the modular functions j and j_{11} which we have already introduced, but it turns out that the coefficients are so large that computation becomes difficult. Instead we will introduce some other modular functions. We omit most of the details.

Our basic method is as follows: given an abstract genus 1 curve E with a given point O, one determines a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

by finding functions x and y on E which have poles of order 2 and 3 at the point O of E, respectively. The Riemann-Roch theorem shows that the space of functions on E with poles of order at most 6 at O and no other poles has dimension exactly 6; since we have the seven functions $y^2, xy, y, x^3, x^2, x, 1$ all with poles of order at most 6 at O and no other poles, they must satisfy a linear relation. Renormalizing x and y one obtains a Weierstrass equation as above; see [14, Chapter 3, Section 3] for details. We must find such functions x and y and then determine the linear relation.

We first exhibit some modular forms of weight 2 for $\Gamma_0(11)$; recall that these are functions $f : \mathcal{H} \to \mathbb{C}$ such that

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right) = (c\tau + d)^2 f(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$. The first is constructed as a *theta series* (see [13, Chapter 7, Section 6] for a similar construction): we let $Q(x, y) = x^2 + xy + 3y^2$ be a quadratic form of discriminant 11 and define $r_Q(n)$ to be the number of integer solutions (x, y) to the equation $Q(x, y) = n$. Set

$$\begin{aligned}\theta_Q(\tau) &= \sum r_Q(n)q^n \\ &= 1 + 2q + 4q^3 + 2q^4 + 4q^5 + 6q^9 + 2q^{11} + 4q^{12} + 8q^{15} + \cdots\end{aligned}$$

where $q = e^{2\pi i\tau}$ as before. One uses the Poisson summation formula to show that

$$\theta_Q\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right) = \pm(c\tau + d)\theta_Q(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$; $\theta_Q^2(\tau)$ is therefore a modular form of weight 2 for $\Gamma_0(11)$.

There is another well known modular form of weight 2 for $\Gamma_0(11)$

$$\begin{aligned}h(\tau) &= q\prod_{n\geq 1}(1 - q^n)^2(1 - q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + \cdots ;\end{aligned}$$

see [7, Chapter 8, Corollary 8.9 and Chapter 9, Section 4, Example 5]. The first modular function we will use is

$$\begin{aligned}F(\tau) &= \frac{\theta_Q^2(\tau)}{h(\tau)} \\ &= \frac{1}{q} + 6 + 17q + 46q^2 + 116q^3 + 252q^4 + 533q^5 + 1034q^6 + 1961q^7 + \cdots\end{aligned}$$

Since both θ_Q^2 and h have weight 2, F will have weight 0 and thus satisfies

$$F\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right) = F(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$. As we saw before, this means that F defines a meromorphic function on the Riemann surface $X_0(11)$.

To obtain a second modular function, we begin with $q\frac{dF}{dq}$, which one easily check (from the fact that F is a modular function) is also modular of weight 2 for $\Gamma_0(11)$. We set

$$\begin{aligned} G(\tau) &= \frac{q\frac{df}{dq}(\tau)}{h(\tau)} \\ &= -\frac{1}{q^2} - \frac{2}{q} + 12 + 116q + 597q^2 + 2298q^3 + 7616q^4 + 22396q^5 + \cdots \end{aligned}$$

As with $F(\tau)$, $G(\tau)$ defines a meromorphic function on $X_0(11)$.

Let us choose to make the cusp $i\infty$ the identity point on the elliptic curve $X_0(11)$. We must find linear combinations of F and G with the required poles at $i\infty$ and no other poles. It is clear from the Laurent series above that F has a pole of order 1 and G has a pole of order 2 at $\tau = i\infty$ (which corresponds to $q = 0$). It is also not too hard to check that F and G have no other poles on $\mathcal{H}$. Unfortunately, it turns out that they do have poles at the cusp $\tau = 0$ (where $q = 1$) and we will have to account for these poles.

We do this using the *Atkin-Lehner involution* w. This is an automorphism of $\mathcal{H}$ given by $\tau \mapsto \frac{-1}{11\tau}$. One checks easily that it is compatible with the action of $\Gamma_0(11)$ on $\mathcal{H}$, so it yields an involution w of $\Gamma_0(11)\backslash\mathcal{H} = X_0(11)$. Note that w interchanges the cusps $\tau = 0$ and $\tau = i\infty$. It can be shown using a trick involving the Poisson summation formula that $F \circ w = F$ and $G \circ w = -G$. To find a candidate function for x, then, we need to find a polynomial $p(u, v)$ such that $p(F, G)$ starts with $\frac{1}{q^2}$ and $p(F, G) \circ w = p(F, -G)$ has no negative powers of q. This is an exercise in linear algebra; one of the simplest such polynomials is $p(u, v) = (u^2 - v - 10v)/2$, which yields

$$\begin{aligned} x &= \frac{1}{q^2} + \frac{2}{q} - 1 + 5q + 8q^2 + q^3 + 7q^4 - 11q^5 + 10q^6 + \cdots \\ x \circ w &= 22 + 242q + 1210q^2 + 4598q^3 + 15246q^4 + 44770q^5 + 121484q^6 + \cdots \end{aligned}$$

We find y in a similar way; the polynomial $p(u, v) = (-uv + u^3 - 10u^2 - 22u)/2$ works and yields

$$\begin{aligned} y &= \frac{1}{q^3} + \frac{8}{q^2} + \frac{17}{q} + 13 + 42q + 66q^2 + 24q^3 + 72q^4 - 70q^5 + \cdots \\ y \circ w &= 121 + 1331q + 7986q^2 + 37268q^3 + 149072q^4 + 531069q^5 + \cdots \end{aligned}$$

To determine the polynomial satisfied by x and y we start with

$$y^2 - x^3 = \frac{10}{q^5} + \frac{89}{q^4} + \frac{287}{q^3} + \frac{506}{q^2} + \frac{1111}{q} + 2606 + 3498q + 4729q^2 + \cdots$$

and successively add multiples of xy, x^2, y and x to cancel off the rest of the poles. Thus the next terms are

$$y^2 - x^3 - 10xy = -\frac{11}{q^4} - \frac{33}{q^3} + \frac{66}{q^2} + \frac{121}{q} - 264 + 198q + \cdots$$

$$y^2 - x^3 - 10xy + 11x^2 = \frac{11}{q^3} + \frac{88}{q^2} + \frac{187}{q} + 143 + 462q + 726q^2 + \cdots$$

$$y^2 - x^3 - 10xy + 11x^2 - 11y = 0$$

We have therefore found the Weierstrass equation

$$y^2 - 10xy - 11y = x^3 - 11x^2.$$

This equation can be written in a different form which is in more common usage: replacing y by $y + 5x - 19$ and x by $x - 5$ yields the standard form

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

5. Rational points on $X_0(11)$

At this point we have found that $X_0(11)$ can be represented by an elliptic curve over $\mathbb{Q}$, and that an equation for this elliptic curve is

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It is easy to determine the torsion subgroup of this curve: it is the group of order 5

$$X_0(11)_{\mathbb{Q}}(\mathbb{Q})_{\text{tors}} = \{O, (5,5), (16,-61), (16,60), (5,-6)\}.$$

The rank of $X_0(11)_{\mathbb{Q}}(\mathbb{Q})$ is more difficult to determine, although there are methods to compute it. One finds (see [2, p. 110] that $X_0(11)_{\mathbb{Q}}(\mathbb{Q})$ has rank 0, so that

$$X_0(11)_{\mathbb{Q}}(\mathbb{Q}) = \{O, (5,5), (16,-61), (16,60), (5,-6)\}.$$

Two of these rational points were expected: they correspond to the cusps. Since $X_0(11)_{\mathbb{Q}}(\mathbb{Q})$ is not the same as $\mathrm{Ell}_0(\mathbb{Q})$, we can not at the moment give good interpretations of the other 3 points. Note that even if they do correspond to elements (E, C) of $\mathrm{Ell}_0(\mathbb{Q})$, we can not be sure whether or not there are any elliptic curves over $\mathbb{Q}$ with rational 11-torsion; indeed, all we would know is that there exists a rational elliptic curve E and a point $P \in E[11]$ such that $\sigma(P)$ is a multiple of P for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

6. Refined modular pairs and $X_1(11)$

Although we developed a good theory of the modular curve $X_0(11)$, it ended up not being quite good enough to answer the question of whether or not there exist elliptic curves over $\mathbb{Q}$ with rational 11-torsion. In order to determine this, we will consider classifying a different collection of pairs: we define a *refined modular pair* over a field K to be an elliptic curve E defined over K together with a point $P \in E(K)$ of exact order 11. Two such pairs (E_1, P_1) and (E_2, P_2) are said to be isomorphic if there exist an isomorphism of E_1 and E_2, defined over K, which sends P_1 to P_2. We will write $\mathrm{Ell}_1(K)$ for the set of isomorphism classes of refined modular pairs (E, P) over K. The question of the existence of rational elliptic curves with rational 11-torsion is precisely the question of whether or not $\mathrm{Ell}_1(\mathbb{Q})$ is nonempty.

As usual, we begin by analyzing $\mathrm{Ell}_1(\mathbb{C})$ using lattices. First one normalizes the lattices to reduce to considering refined modular pairs of the form $(\mathbb{C}/\Lambda_\tau, \frac{1}{11})$ with

$\tau \in \mathcal{H}$. Proceeding as with $\mathrm{Ell}_0(\mathbb{C})$, one finds that two such pairs $(\mathbb{C}/\Lambda_\tau, \frac{1}{11})$ and $(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{11})$ are isomorphic if and only if there is a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \tau',$$

and $a, d \equiv 1 \pmod{11}$ and $c \equiv 0 \pmod{11}$. We will write $\Gamma_1(11)$ for the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of such matrices; our results to this point are that there is a bijection

$$\begin{aligned} \Gamma_1(11)\backslash\mathcal{H} &\longleftrightarrow \mathrm{Ell}_1(\mathbb{C}) \\ \tau &\longrightarrow \left(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\right) \end{aligned}$$

$\Gamma_1(11)$ turns out to be a significantly more complicated group than $\Gamma_0(11)$, and there is no particularly simple fundamental domain for $\Gamma_1(11)\backslash\mathcal{H}$. However, it is still possible to do a little combinatorial algebra and compute what $\Gamma_1(11)\backslash\mathcal{H}$ should look like: it turns out that we need to adjoin a set $\mathcal{C}_1$ of 10 cusps to $\Gamma_1(11)\backslash\mathcal{H}$ to obtain a compact Riemann surface which we denote $X_1(11)$:

$$X_1(11)(\mathbb{C}) \longleftrightarrow \mathrm{Ell}_1(\mathbb{C}) \cup \mathcal{C}_1.$$

In fact, with the proper machinery (primarily involving a fairly well developed theory of the modular functions for $\Gamma_1(11)$; see [5, Example 9.1.6]) it can be shown that $X_1(11)$ still has genus 1. Methods similar to those we discussed for $X_0(11)$ can also be used to show that $X_1(11)$ can be defined as an algebraic curve $X_1(11)_{\mathbb{Q}}$ over $\mathbb{Q}$: for example, in the notation of Section 4, $X_1(11)_{\mathbb{Q}}$ can be realized as the curve associated to the fixed field of $\mathbb{Q}(t, E[11])$ by

$$H_1 = \left\{ \begin{pmatrix} a & 0 \\ b & \pm 1 \end{pmatrix} \mid a \in (\mathbb{Z}/11\mathbb{Z})^*, b \in \mathbb{Z}/11\mathbb{Z} \right\},$$

considered as a subgroup of $\mathrm{Gal}(\mathbb{Q}(t, E[11])/\mathbb{Q}(t))$. As always, we still have the interpretation

$$X_1(11)_{\mathbb{Q}}(\mathbb{C}) \longleftrightarrow \mathrm{Ell}_1(\mathbb{C}) \cup \mathcal{C}_1.$$

However, there is an unexpected complication in this rational structure: not all of the cusps actually lie in $X_1(11)_{\mathbb{Q}}(\mathbb{Q})$. In fact, it turns out that 5 of the cusps lie in this group, while the other 5 are defined over the maximal real subfield $\mathbb{Q}(\zeta_{11})^+$ of $\mathbb{Q}(\zeta_{11})$; this is a degree 5 extension of $\mathbb{Q}$. It follows that for a general field K containing $\mathbb{Q}$, $X_1(11)_{\mathbb{Q}}(K)$ contains either 5 or 10 cusps, depending on whether or not K contains $\mathbb{Q}(\zeta_{11})^+$. See [5, Example 9.3.5] for a discussion.

7. Moduli spaces

The key to determining whether or not there exist elliptic curves over $\mathbb{Q}$ with rational 11-torsion is an understanding of the relationship between the $\mathbb{Q}$-rational points of $X_1(11)_{\mathbb{Q}}$ and $\mathrm{Ell}_1(\mathbb{Q})$. We constructed $X_1(11)$ so that its non-cuspidal complex points correspond to $\mathrm{Ell}_1(\mathbb{C})$, but it is not at all clear if the same interpretation should hold over $\mathbb{Q}$.

This question is an example of a very important sort of problem in modern algebraic geometry called a *moduli problem*. Let $F(K)$ be some sort of set of geometric objects over a field K; for example, $F(K)$ could be

- isomorphism classes of elliptic curves E over K;
- isomorphism classes of modular pairs (E, C) over K;
- isomorphism classes of refined modular pairs (E, P) over K;
- isomorphism classes of algebraic curves of genus 2 over K;
- algebraic surfaces embedded in $\mathbb{P}^3_K$;

or any other similar sort of set. The key thing is that F should be defined for every field K (say, of characteristic 0) and that for every inclusion of fields $K \hookrightarrow L$ there should be a *restriction map*

$$F(K) \to F(L)$$

such that for any tower of fields $K \hookrightarrow L \hookrightarrow M$, the composition of the restriction maps $F(K) \to F(L)$ and $F(L) \to F(M)$ is just the restriction map $F(K) \to F(M)$. (In all of the examples above the restriction map is the obvious one reinterpreting an object defined over K as defined over L.) F is an example of a *functor* from the category of fields of characteristic 0 to the category of sets.

The goal is to find a nice geometric object (say, a projective variety defined over $\mathbb{Q}$) X such that for every field K there is a bijection

$$X(K) \longleftrightarrow F(K).$$

(It should also be compatible with the restriction maps $X(L) \to X(K)$ and $F(L) \to F(K)$.) We have never actually been able to do this, even over $\mathbb{C}$; we always had to add a few extra points (the cusps) in order to fill in some holes. This situation turns out to be very common; let us agree to allow a "small" exceptional set of points as well.

If we could find such an X, we would suddenly have a powerful tool with which to study F. For example, if we could find such an X for Ell_1, then the question of the existence of elliptic curves with 11-torsion becomes a question about rational points on a single variety. This philosophy of using geometric objects to study whole families of other geometric objects is fundamental in modern algebraic geometry; such an X is called a *fine moduli space* for F.

Unfortunately, fine moduli spaces do not exist for all F. In fact, they are fairly rare. One simple necessary condition for the existence of such a moduli space X for F is that the restriction maps $F(K) \to F(L)$ be injective for all inclusions $K \hookrightarrow L$; this is because the maps $X(K) \to X(L)$ are obviously injective, and $F(K) \to F(L)$ must agree with this map. This immediately shows that $F = \mathrm{Ell}$ has no fine moduli space: indeed, take $K = \mathbb{Q}$ and $L = \bar{\mathbb{Q}}$. There are many elliptic curves over $\mathbb{Q}$ which are not isomorphic over $\mathbb{Q}$ but which have the same j-invariant. Since they have the same j-invariant, they become isomorphic over $\bar{\mathbb{Q}}$; therefore, these elliptic curves have the same image under $\mathrm{Ell}(\mathbb{Q}) \to \mathrm{Ell}(\bar{\mathbb{Q}})$, so it is not injective and no fine moduli space can exist.

If F does not have a fine moduli space, it still could happen that it has a *coarse moduli space*. This is a projective variety X such that for every K there is a map

$$F(K) \to X(K)$$

which satisfies certain technical properties, but which need not be an isomorphism. This is what $X(1)_{\mathbb{Q}}$ and $X_0(11)_{\mathbb{Q}}$ are for Ell and Ell_0. Coarse moduli spaces are also useful, but it requires more care to obtain information about F from them. In the case of Ell_0, the points $X_0(11)_{\mathbb{Q}}(K)$ turn out to correspond to modular pairs (E, C)

defined over K, but only up to isomorphism over $\bar{K}$. In particular, the natural map

$$\mathrm{Ell}_0(K) \to X_0(11)_{\mathbb{Q}}(K) - \mathcal{C}_0$$

is surjective but need not be injective. Even given this, the existence of rational points on $X_0(11)_{\mathbb{Q}}$ does not imply the existence of elliptic curves over $\mathbb{Q}$ with rational 11-torsion; for the cyclic subgroup C to be defined over $\mathbb{Q}$ means only that it is mapped to itself under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, not that it is actually pointwise fixed.

Remarkably, $X_1(11)_{\mathbb{Q}}$ turns out to be a fine moduli space for Ell_1 (once we have taken into account the cusps). That is, for every field K containing $\mathbb{Q}$ there is a bijection

$$X_1(11)_{\mathbb{Q}}(K) \longleftrightarrow \mathrm{Ell}_1(K) \cup \mathcal{C}(K)$$

where we remember that $\mathcal{C}(K)$ contains either 5 or 10 cusps depending on whether or not K contains $\mathbb{Q}(\zeta_{11})^+$.

These facts are quite difficult to prove. The standard references are [4] and [6], but they both require a great deal of algebraic geometric background. There is a nice summary in [5, Part 2], although even it requires a fair amount of algebraic geometry.

We give a brief indication of why $X_1(11)_{\mathbb{Q}}$ is better behaved than our other examples. The key fact turns out to be the following rigidity statement (see [6]; this particular section requires only familiarity with the material of [14, Chapter 3]): If (E_1, P_1) and (E_2, P_2) are refined modular pairs defined over a field K, then there is at most one isomorphism $E_1 \cong E_2$ sending P_1 to P_2.

Given this, we can show that the restriction maps $\mathrm{Ell}_1(K) \to \mathrm{Ell}_1(L)$ are injective for extensions $K \subseteq L$, so that at least that obstruction to the existence of a fine moduli space is avoided. Unwinding the definitions, we must prove that if (E_1, P_1) and (E_2, P_2) are modular pairs over K for which there exists an isomorphism $\varphi : E_1 \to E_2$ defined over L with $\varphi(P_1) = P_2$, then φ is actually defined over K. Let σ be any element of $\mathrm{Gal}(L/K)$. Acting on everything by σ, we obtain an isomorphism $\varphi^\sigma : E_1^\sigma \to E_2^\sigma$ sending $\sigma(P_1) \to \sigma(P_2)$; here by E_i^σ we mean the elliptic curve with equation given by acting on an equation of E_i by σ. But since E_1 and E_2 are defined over K, σ does not effect their defining equations at all, and $E_1^\sigma = E_1$, $E_2^\sigma = E_2$. The same is true of P_1 and P_2, so we see that φ^σ yields an isomorphism of modular pairs over L $(E_1, P_1) \cong (E_2, P_2)$. By rigidity this must agree with φ, so $\varphi = \varphi^\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$. But by the main theorem of Galois theory (more or less) this means that φ is defined over K, which is what we were trying to show.

8. The elliptic curve $X_1(11)_{\mathbb{Q}}$

Given what we said in the last section, to determine whether or not there exists a rational elliptic curve with rational 11-torsion is the same as determining whether or not there are non-cuspidal rational points on $X_1(11)_{\mathbb{Q}}$. To do this, we must find an equation for $X_1(11)_{\mathbb{Q}}$. This can be done in principal as we did for $X_0(11)_{\mathbb{Q}}$, although it is more complicated; in any event, one finds the equation

$$y^2 + y = x^3 - x^2.$$

This elliptic curve has 5 torsion points:

$$X_1(11)_{\mathbb{Q}}(\mathbb{Q})_{\mathrm{tors}} = \{O, (0,0), (1,-1), (1,0), (0,-1)\}.$$

The rank of $X_1(11)_{\mathbb{Q}}$ is, as always, more difficult to determine. By [2, p. 110], it can be shown to have rank 0. Thus,

$$X_1(11)_{\mathbb{Q}}(\mathbb{Q}) = \{O, (0,0), (1,-1), (1,0), (0,-1)\}.$$

So $X_1(11)_{\mathbb{Q}}$ has exactly five rational points. But recall that we expected five rational cusps! Thus $X_1(11)_{\mathbb{Q}}$ has no non-cuspidal rational points; $\mathrm{Ell}_1(\mathbb{Q})$ is therefore empty, and we conclude that there are no elliptic curves over $\mathbb{Q}$ with rational points of order 11!

9. Generalizations

Of course, very little specific to the number 11 came into our construction of $X_0(11)_{\mathbb{Q}}$ and $X_1(11)_{\mathbb{Q}}$. One can construct such curves $X_0(N)_{\mathbb{Q}}$ and $X_1(N)_{\mathbb{Q}}$ for any positive integer N, corresponding to pairs of elliptic curves and cyclic subgroups of order N and elliptic curves and points of order N, respectively. For $N \geq 4$ it turns out that $X_0(N)_{\mathbb{Q}}$ is a coarse moduli space and $X_1(N)_{\mathbb{Q}}$ is a fine moduli space.

It follows that to determine whether or not there exist elliptic curves over $\mathbb{Q}$ with a point of order N, "all" we have to do is determine whether or not $X_1(N)_{\mathbb{Q}}$ has non-cuspidal rational points. Unfortunately, as N increases the genus of $X_1(N)_{\mathbb{Q}}$ increases and the methods we used for $N = 11$ fail to work.

It has been known for quite a while that for $N = 1,2,3,4,5,6,7,8,9,10,12$, $X_1(N)_{\mathbb{Q}}$ has genus 0 and therefore is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. (In general, a curve of genus 0 over $\mathbb{Q}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ if and only if it has a rational point. In these cases, the cusps always give automatic rational points.) It follows that there exist infinitely many rational elliptic curves with points of order $1,2,3,4,5,6,7,8,9,10,12$.

For higher N the problem is much more difficult. Before 1977, results were known only for a few values of N, such as $N = 11, 13$. This all changed when Barry Mazur succeeded in fully analyzing the rational points on these curves, yielding the following remarkable theorem.

Theorem 9.1 (Mazur [8] [9]). *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup of $E(\mathbb{Q})$ is one of the following* 15 *groups:*

$$\mathbb{Z}/N\mathbb{Z} \quad (N=1,2,3,4,5,6,7,8,9,10,12);$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \quad (N=1,2,3,4).$$

More recent work on the points of $X_1(N)$ over larger number fields has yielded the following theorem.

Theorem 9.2 (Merel [10]). *Let K be a number field of degree d. Then there is an integer M, depending only on d (and not on K itself) such that every elliptic curve over K has torsion subgroup of order at most M.*

References

[1] Gary Cornell, Joseph Silverman and Glenn Stevens (ed.), *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997.
[2] J.E. Cremona, *Algorithms for Modular Elliptic Curves*. Cambridge University Press, Cambridge, 1997.
[3] Pierre Deligne and W. Kuyk (ed.), *Modular forms of one variable II*. Lecture notes in mathematics 349, Springer-Verlag, Berlin, 1973.
[4] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*. In [3].
[5] Fred Diamond and John Im, *Modular forms and modular curves*. In [11], pp. 39-133.

[6] Nicholas Katz and Barry Mazur, *Arithmetic moduli of elliptic curves.* Princeton University Press, Princeton, New Jersey, 1985.

[7] Anthony Knapp, *Elliptic curves.* Princeton University Press, Princeton, New Jersey, 1992.

[8] Barry Mazur, *Modular curves and the Eisenstein ideal.* IHES Publications Mathématiques, vol. 47 (1977), pp. 33-186.

[9] Barry Mazur, *Rational isogenies of prime degree.* Inventiones Mathematicae, vol. 44 (1978), pp. 129-162.

[10] Loic Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Inventiones Mathematicae, vol. 124 (1996), pp. 437-449.

[11] V. Kumar Murty (ed.), *Seminar on Fermat's last theorem.* American Mathematical Society, Providence, Rhode Island, 1995.

[12] David Rohrlich, *Modular curves, Hecke correspondences and L-functions.* In [1], pp. 41-100.

[13] Jean-Pierre Serre, *A Course in Arithmetic.* Springer-Verlag, New York, 1973.

[14] Joseph Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[15] Joseph Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1994.