MODULI OF ELLIPTIC CURVES

JAMES PARSON

1. Introduction

The purpose of these notes is to provide a quick introduction to the moduli of elliptic curves. There are many excellent and thorough references on the subject, ranging from the slightly archaic [Igu59] and [Shi94] to the more difficult [KM85] and [DR73]. Brian's forthcoming book on the Ramanujan conjecture also covers some of this material and includes a careful comparison of the transcendental and algebraic theories. In order to read Mazur's paper [Maz78], it is not necessary to consider many of the subtle issues of the subject; indeed, all we will need to understand for the time being is how to construct good arithmetic models of $Y_1(N)/\mathbf{C}, X_1(N)/\mathbf{C}$, and the associated modular correspondences over $\mathbf{Z}[1/N]$.

In order to have a concrete example or two to keep in mind, let us start by recalling the Tate normal form that was introduced in Bryden's lecture. He discussed it in the following context: let K be a field and let E/K be an elliptic curve. Fix a point $P \in E(K)$ such that P does not have order 1, 2, or 3. Bryden explained that there is a unique isomorphism of the pair $(E/K, P)$ to a pair $(E(b,c)/K, (0,0))$, where b and c are in K and $E(b,c)$ is given by the Weierstrass equation

$$E(b,c) : y^2 + (1-c)xy - by = x^3 - bx^2.$$

For future reference, let me note that the discriminant of this Weierstrass cubic is

$$\Delta(b,c) = (1-c)^4b^3 - (1-c)^3b^3 - 8(1-c)^2b^4 + 36(1-c)b^4 - 27b^4 + 16b^5.$$

Conversely, for any $(b,c) \in K^2$ such that $\Delta(b,c) \in K^\times$, the pair $(E(b,c),(0,0))$ is an elliptic curve with a point not of order 1, 2, or 3. In other words, the set of isomorphism classes of such pairs (E,P) has been put in bijection with $\{(b,c) : \Delta(b,c) \in K^\times\}$, the set of K-points of $\mathbf{A}^2 - \{\Delta = 0\}$, by means of the Tate-normal-curve construction. Note, moreover, that these bijections for variable K are functorial in injections of fields $K \to K'$. An informal (for now) way to describe these properties of $E(b,c)$ is to say that the pair $(E(b,c),(0,0))$ over $\mathbf{A}^2 - \{\Delta = 0\}$ is the universal pair of an elliptic curve and a point not of order 1, 2, or 3.

In fact, the results of the previous paragraph can be improved, replacing the field K (or rather $\mathrm{Spec}(K)$) with an arbitrary scheme S throughout. To be precise, consider pairs $(E/S, P)$, where E/S is an elliptic curve (i.e. an abelian scheme of relative dimension 1) and $P \in E(S)$ a section such that the image of P in each geometric fiber of E/S does not have order 1, 2, or 3. Then there are $b, c \in \Gamma(S, \mathcal{O}_S)$ and a unique isomorphism of $(E/S, P)$ with $(E(b,c)/S, (0,0))$; conversely, for any $b, c \in \Gamma(S, \mathcal{O}_S)$ such that $\Delta(b,c) \in \Gamma(S, \mathcal{O}_S)^\times$, the pair $(E(b,c)/S, (0,0))$ is an elliptic curve with a section not of order 1, 2, or 3 in any geometric fiber. The justification for this claim is in §9.

As in Bryden's discussion, the Tate normal form can be used to study the particular case, say, when the point P has exact order 5. The addition law provides the following universal formulas:

$$\begin{aligned} [1]P &= (0,0) & [-1]P &= (0,b) \\ [2]P &= (b,bc) & [-2]P &= (b,0) \\ [3]P &= (c,b-c) & [-3]P &= (c,c^2) \end{aligned}$$

Consequently, the point P has exact order 5 (or, equivalently, $[-2]P = [3]P$) if and only if $b = c$. In other words, for any pair $(E/K, P)$ consisting of an elliptic curve and a point P of exact order 5 in $E(K)$, there is a unique isomorphism to a pair $(E(b,b),(0,0))$ for some $b \in K$ such that $\Delta(b,b) = b^5(b^2 - 11b - 1) \in K^\times$; conversely, for any such b, the pair $(E(b,b),(0,0))$ is an elliptic curve with a point of exact order 5. As with

$E(b,c)$ above, these results can be strengthened to hold when $\operatorname{Spec}(K)$ is replaced by a scheme S. Once again, the details can be found in §9.

For comparison, it may be helpful to keep the exact-order-4 case in mind as well: the point P has exact order 4 if and only if $c = 0$, and so the universal curve is $E(b,0)$ over $\mathbf{A}^1 - \{\Delta(b,0) = 0\}$. (Note that $\Delta(b,0) = b^4(1+16b)$.)

Before continuing, let us pluck a bit of fruit:

Proposition 1.1. *Let R be a discrete valuation ring with quotient field K and residue field k of characteristic $\neq 5$. Let E/K be an elliptic curve with potentially good reduction and $P \in E(K)$ be a point of exact order 5. Then E/K has good reduction.*

Proof. By the above discussion applied to $(E/K, P)$, there is a unique $b \in K$ with $\Delta(b,b) \in K^\times$ such that $(E/K, P) = (E(b,b), (0,0))$. In order to see that E/K has good reduction, it would suffice to see that $b \in R$ and $\Delta(b,b) \in R^\times$, since then $(E(b,b),(0,0))$ would define an elliptic curve over $\operatorname{Spec}(R)$ extending E/K.

To say that E/K has potentially good reduction means that there is a finite separable extension K'/K such that E/K' has good reduction; in other words, if R' is the integral closure of R in K', then E/K' extends to an elliptic curve E/R'. Since K'/K is separable, the ring R' is a semi-local Dedekind domain, and so the point $P \in E(K) \subset E(K')$ extends to a section $P \in E(R')$, as E/R' is proper. Letting k' be any quotient of R' that is a field, we see that the image of P in $E(k')$ must have exact order 5, since $\ker(E(R') \to E(k'))$ contains no 5-torsion, as the characteristic of k' is not 5.

Because the pair $(E/K', P)$ extends to a similar structure over R', it must be that $b \in R'$ and $\Delta(b,b) \in R'^\times$. It follows from $R' \cap K = R$ that $b \in R$ and $\Delta(b,b) \in R^\times$, as desired. □

One can have a bit of fun with the formulas, using them to find interesting curves with small conductor. For instance, in the $N = 5$ case, one can look for the choices of integer b that make $\Delta(b,b) = b^5(b^2 - 11b - 1)$ as simple as possible, setting, say, $b^5 = 1$ or $b^2 - 11b - 1 = -1$. These choices give $E(1,1) : y^2 - y = x^3 - x$ with discriminant $\Delta(1,1) = -11$ and $E(11,11) : y^2 - 10xy - 11y = x^3 - 11x^2$ with discriminant $\Delta(11,11) = -11^5$, which are known to be isomorphic to the curves $J_1(11)$ and $J_0(11)$. (This fact is proved below in §8.) In the case $N = 4$, one chooses $b = 1$ to make $\Delta(b,0) = b^4(1+16b)$ simple and finds $E(1,0) : y^2 + xy - y = x^3 - x^2$ with $\Delta(1,0) = 17$, which is known to be isogeneous to $J_0(17)$ (but this curve is not $J_0(17)$, since the component group of the modulo-17 fiber of the Néron model of $J_0(17)$ is known to have four components, whereas the same fiber of the Néron model of $E(1,0)$ is connected). Choosing $b = -1$ gives the nice curve $E(-1,0) : y^2 + xy + y = x^3 + x^2$ with $\Delta(-1,0) = -15$, which is isogeneous to $J_0(15)$.

2. Digression on representable functors

The essential fact about elliptic curves with a 5-torsion point sketched in the above paragraphs is that for any scheme S, there is a bijection between, on the one hand, isomorphism classes of pairs (E,P) of an elliptic curve E/S and a section P of exact order 5 in all geometric fibers and, on the other hand, the S-points of the affine scheme $Y = \operatorname{Spec}(\mathbf{Z}[T, 1/\Delta(T,T)])$. These bijections are moreover functorial in maps $S \to S'$ of schemes. (The reader may be tempted to restrict to $\mathbf{Z}[1/5]$-schemes, but this is unnecessary for the moment. An application of working over $\mathbf{Z}$ can be found in §8.) All of this can be stated succinctly by saying that there is a natural isomorphism between the contravariant functor $F : (\text{Schemes}) \to (\text{Sets})$ defined by

$$F(S) = \{(E,P) : E/S \text{ is an elliptic curve}, P \in E(S) \text{ has exact order 5 in all geometric fibers}\}/\approx$$

and the contravariant functor of S-points of Y.

In general, if F is a contravaraint functor from a category A to a category B, one says that F is *representable* if there is an object Y of A and a natural isomorphism $i : \operatorname{Hom}(\cdot, Y) \Rightarrow F$; one then says that (Y,i) represents F—it is important to keep track of the natural isomorphism i, of course, and not just Y. Yoneda's lemma, which is a bit of psychologically helpful category-theory formalism, tells us that if (Y,i) and (Y',i') both represent F, there is a unique isomorphism $f : Y \to Y'$ such that $i' \circ f = i$. (Explicitly, the map f corresponds to $i'^{-1}(i(\mathrm{id}_Y))$.) This fact is what we use to pin down the arithmetic models of modular curves, at least of $Y_1(N)$ and $X_1(N)$ for $N \geq 4$: they will be described as objects representing certain functors, which determines them up to unique isomorphism.

In the concrete case above of elliptic curves and 5-torsion points, the representability of the functor F is established by means of the universal object $(E(T,T),(0,0))$: for any scheme S and morphism $S \to Y$, one can pull back the object $(E(T,T),(0,0))$ to give a similar structure over S; one then proves that the induced map $Y(S) \to F(S)$ is a bijection. This picture is a general aspect of representable functors: returning to the general situation of $F : A \to B$, one obtains for any object Y and $y \in F(Y)$ a natural transformation $i : Y \Rightarrow F$ given by pulling back y along any S-valued point $S \to Y$, just as in the concrete case. If this natural transformation is a natural isomorphism, then (Y,i) represents F, and the pair (Y,y) can be understood as a universal structure for the functor F. Conversely, if (Y,i) represents F, then there is a $y \in F(Y)$ giving rise to i as above (i.e. a y such that (Y,y) is a universal structure); one may take y to be $i(\mathrm{id}_Y) \in F(Y)$, because $f = \mathrm{id}_Y \circ f$ for any $f : S \to Y$.

The conclusion of the previous paragraph is that in place of the pair (Y,i), one could just as well take the equivalent data (Y,y): to have a universal structure (Y,y) for the functor F is the same as to represent F. This universal-structure picture is generally the way that representability will be used in what follows.

3. The curves $Y_1(N)$ in general

With the above terminology in mind, we turn to the curves $Y_1(N)$ in general (or at least for $N \geq 4$). The functor that will be used to describe the arithmetic model of $Y_1(N)$ is $F_N : (\text{Schemes}/\mathbf{Z}[1/\text{N}]) \to (\text{Sets})$ defined by

$$F_N(S) = \{(E,P) : E/S \text{ is an elliptic curve}, P \in E(S) \text{ has exact order } N \text{ in all geometric fibers}\}/\approx .$$

In §9, the following is proved

Proposition 3.1. *For $N \geq 4$, the functor F_N is represented by a scheme $Y_1(N)/\operatorname{Spec}(\mathbf{Z}[1/N])$ and its universal elliptic curve with section of exact order N.*

The functor F_N could certainly be defined on arbitrary schemes and as such would even be representable, but the object that represents the extended functor is not all of what one would want to call $Y_1(N)/\operatorname{Spec}(\mathbf{Z})$, which is why the domain is restricted to $\mathbf{Z}[1/N]$-schemes. (This behavior is discussed in more detail in §5.) It is quite important to identify $Y_1(N)(\mathbf{C})$ (with its analytic topology) with the Riemann surface $\Gamma_1(N)\backslash\mathbf{H}$; the construction of such an identification will not be discussed here. The argument starts with the Weierstrass elliptic curve

$$Y^2 = X^3 + g_4(\tau)X + g_6(\tau)$$

over $\mathbf{H}$, which is *relatively algebraic* in that it is defined by polynomial equations whose coefficients are holomorphic functions on $\mathbf{H}$—the coefficients are even modular forms. From this beginning, one must be somewhat careful to prove the claim, but nothing too serious is involved.

Before discussing the properties of $Y_1(N)$, let us see briefly why F_1 is not representable. The set $F_1(S)$ is simply the isomorphism classes of elliptic curves over S. The twisting construction shows that the map $F_1(\operatorname{Spec}(\mathbf{Q})) \to F_1(\operatorname{Spec}(\mathbf{C}))$ is not injective; if, however, F_1 were a representable functor, it would have to be injective. The source of the twisting, which obstructs representability, is the existence of non-trivial automorphisms of elliptic curves ($[-1]$, for example); more generally, functors that classify isomorphism classes of objects tend not to be representable when those objects have non-trivial automorphisms, since such automorphisms often allow one to construct twists. The reader should consider how the existence of appropriate twists shows similarly that F_2 and F_3 are not representable.

Here is the main fact one can prove about $Y_1(N)$ without introducing $X_1(N)$:

Proposition 3.2. *$Y_1(N)/\mathbf{Z}[1/N]$ is smooth and of pure relative dimension 1.*

Proof. The smoothness, at least, seems impossible to check from the construction using Tate normal form discussed below. Both properties can be verified easily by studying the functor F_N, and the work is left to the reader: the smoothness follows from the functorial criterion for smoothness, which is verified easily in this case; similarly, one can compute that the tangent spaces at points in the geometric fibers are 1-dimensional. □

The proposition makes it reasonable to call $Y_1(N)$ a curve over $\mathbf{Z}[1/N]$ and even an arithmetic model of $Y_1(N)/\mathbf{C}$. The next natural question to ask about $Y_1(N)/\mathbf{Z}[1/N]$ would be whether the geometric fibers are connected. Granting the claim above that $Y_1(N)(\mathbf{C})$ is the Riemann surface $\Gamma_1(N)\backslash\mathbf{H}$, it follows that all characteristic-0 fibers have this property. In order to see connectedness for all geometric fibers over $\mathbf{Z}[1/N]$, though, it seems necessary to construct a good compactification $X_1(N)/\mathbf{Z}[1/N]$, as described in the next section. With this compactification available, the connectedness follows from the Stein factorization and the connectedness of characteristic-0 geometric fibers.

Incidentally, by the same argument as in the $N = 5$ case, one deduces the following:

Proposition 3.3. *Let R be a discrete valuation ring with residue characteristic not dividing $N \geq 4$. Let K be its quotient field. Let E/K be an elliptic curve, $P \in E(K)$ be a point of exact order N, and suppose that E/K has potentially good reduction. Then E/K has good reduction.*

The proposition can also be proved using the criterion of Néron-Ogg-Shafarevich without introducing moduli spaces.

4. The compactification $X_1(5)$

I know two general methods for constructing arithmetic models of the compactifications of modular curves. The first method is Igusa's (cf. [Igu59] and [KM85]): it is based on the fact that the j-invariant construction gives a map $Y_1(N) \to \mathbf{A}^1_{\mathbf{Z}[1/N]}$. The target is compactified by $\mathbf{A}^1 \hookrightarrow \mathbf{P}^1$, and $X_1(N)$ is defined as the normalization of $\mathbf{P}^1_{\mathbf{Z}[1/N]}$ in the fraction field of $Y_1(N)/\mathbf{Q}$. One studies the behavior of $X_1(N)$ over the section ∞ of $\mathbf{P}^1$ by using degenerating families of elliptic curves. This construction is somewhat unsatisfying, since although $Y_1(N)$ is constructed to represent a moduli problem, the scheme $X_1(N)$ does not appear as any sort of parameter space.

The second method is that of [DR73], which produces a moduli functor on $\mathbf{Z}[1/N]$-schemes (like F_N in §3) represented by a proper, smooth curve $X_1(N)/\mathbf{Z}[1/N]$. In order to get a sense for what this moduli functor might be, let us return to the example of $Y_1(5)$. This curve has been realized as $\operatorname{Spec}\mathbf{Z}[1/5, T, 1/\Delta(T,T)]$, which is an open subscheme of $\mathbf{A}^1/\mathbf{Z}[1/5]$; the compactification $X_1(5)$ ought to be $\mathbf{P}^1/\mathbf{Z}[1/5]$. Keep in mind that $\Delta(T,T) = T^5(T^2 - 11T - 1)$, and so one can think of the compactification as filling in the sections of $\mathbf{P}^1$ at 0, ∞, and over $\operatorname{Spec}(\mathbf{Z}[1/5, T]/(T^2 - 11T - 1))$.

Let us see how the universal structure $(E(T,T), (0,0))$ degenerates over the complement of $Y_1(5)$. First note that the Weierstrass cubic $E(T,T)$ has fibers that are either smooth or nodal over all of $\operatorname{Spec}(\mathbf{Z}[1/5, T])$. (Concretely, for any field K of characteristic $\neq 5$ and $b \in K$, the curve $E(b,b)$ is either a nodal cubic or smooth.) Moreover, over $\operatorname{Spec}(\mathbf{Z}[1/5, T, 1/T])$, the section $(0,0)$ of $E(T,T)$ lies in the smooth locus. (Concretely, with K, b as above, if $b \in K^\times$, then $(0,0)$ is a smooth point of $E(b,b)$.) Furthermore, this section has exact order 5 in each geometric fiber, using the standard extension of the group law to the smooth locus (cf. [DR73]).

These last observations suggest a generalized moduli problem $G_5 : (\text{Schemes}/\mathbf{Z}[1/5]) \to (\text{Sets})$ with $G_5(S) =$ isomorphism classes of $(E/S, O, P)$, where E/S is proper and flat with fibers that are either smooth genus-1 curves or nodal cubics, where $O, P \in E^{\text{sm}}(S)$ are sections in the smooth locus of E/S, and where, making E^{sm}/S a group scheme using O as the identity section, the section P has exact order 5 in all geometric fibers. One can check (using the same technique as in §9) that G_5 is represented by $\operatorname{Spec}(\mathbf{Z}[1/5, T])$ with universal family $(E(T,T), O, (0,0))$. (Here O is the section at infinity of the Weierstrass cubic $E(T,T)$.) This scheme is a partial compactification of $Y_1(5)$, but it is still missing the two cusps 0 and ∞.

As noted above, the family $E(T,T)$ extends to a family of elliptic curves and nodal cubics over all of $\operatorname{Spec}\mathbf{Z}[1/5, T]$, but at $T = 0$ the section $(0,0)$ degenerates into the singular locus. (Concretely, for any field K, the curve

$$E(0,0) : y^2 + xy = x^3$$

is a nodal cubic with singularity at $(0,0)$.) As for ∞, one can extend the family $E(T,T)$ over $\mathbf{A}^1$ to a family over $\mathbf{P}^1$ as follows: let $T' = 1/T$, so that, working over $\mathrm{Spec}(\mathbf{Z}[1/5, T, 1/T])$, one has

$$E(T,T) : y^2 + \left(1 - \frac{1}{T'}\right) xy - \frac{1}{T'} y = x^3 - \frac{1}{T'} x^2.$$

Making a standard (u, r, s, t) change of variables with $u = T'$ and $r = s = t = 0$ (which sends the section $(0,0)$ to the section $(0,0)$) gives a new Weierstrass equation

$$y^2 + (T' - 1)xy - T'^2 y = x^3 - T'x^2,$$

which determines a curve isomorphic to $E(T,T)$ (over $\mathrm{Spec}(\mathbf{Z}[1/5, T, 1/T])$. This curve evidently extends over $\mathbf{Z}[1/5, T']$, and by gluing this curve and $E(T,T)$, we get a curve C over $\mathbf{P}^1/\mathbf{Z}[1/5]$ (with section $(0,0)$). Setting $T' = 0$ above, we see that the curve degenerates into a nodal cubic at $T' = 0$ (i.e. $T = \infty$), and that the section $(0,0)$ degenerates to the singularity, just as at $T = 0$. (Note, incidentally, that $(C/\mathbf{P}^1_{\mathbf{Z}[1/5]}, O, (0,0))$ is an abstract Weierstrass curve that does not have a global Weierstrass equation.)

Before continuing the analysis of the degeneration at 0 and ∞, let us give an application of what has come so far:

Proposition 4.1. *Let R be a discrete valuation ring of residue characteristic not dividing 5. Let K be the quotient field of R. Let E/K be an elliptic curve and $P \in E(K)$ be a point of exact order 5. Then E/K has stable—i.e. good or multiplicative— reduction.*

Proof. The pair $(E/K, P)$ gives an element of

$$Y_1(5)(K) \subset X_1(5)(K) = X_1(5)(R).$$

Pulling back the family $(C, (0,0))$ over $X_1(5)$ to $\mathrm{Spec}(R)$ gives a model of E/K with special fiber either an elliptic curve or a nodal cubic. □

Returning to the analysis of the degenerations at 0 and ∞, note that the fibers of $(C, (0,0))$ over the sections 0 and ∞ are isomorphic. (Look at the equations.) This means that $(C, (0,0))$ cannot be the universal family for any reasonable moduli problem. To get a hint for how this structure should be refined, consider $Y_1(5)/\mathbf{Q}$. One can ask what the minimal regular model of $E(T,T)$ is at $T = 0$ over $X_1(5)/\mathbf{Q}$. Tate's algorithm tells us that since $E(T,T)$ has semi-stable reduction at $T = 0$ and $\Delta(T,T)$ has a zero of order 5 at $T = 0$, the geometric fiber of this model at $T = 0$ is a pentagon whose sides are $\mathbf{P}^1$'s. Such a structure is called a 5-*gon* in [DR73]; the analogous term for a nodal cubic is a 1-*gon.* In general, a d-gon over an algebraically closed field is anything isomorphic to a loop of $\mathbf{P}^1$'s obtained by gluing ∞ in one copy of $\mathbf{P}^1$ to 0 in the next copy.

Continuing the analysis of the degeneration of $E(T,T)$ at $T = 0$, consider the extension of the sections O and $P = (0,0)$ to the minimal regular model. They necessarily factor through the smooth locus by regularity. (This fact is explained in Brian's notes.) In [DR73] it is proved that there is a unique extension of the group structure on $E(T,T)/Y_1(5)$ (still over $\mathbf{Q}$) to the smooth locus of the minimal regular model at $T = 0$; moreover, one sees easily that P must have exact order 5 in the fiber at 0. (The situation is parallel at ∞.) In sum, this analysis points to the moduli problem considered in [DR73] to define $X_1(5)$: elliptic curves are allowed to degenerate either to 1-gons (as over $T^2 - 11T - 1$), or to 5-gons (as over $T = 0, \infty$), and the section P extends to a section (of exact order 5) of the smooth locus of the degenerating family. A precise statement will be given in the next section.

The most important features of $X_1(5)$ to keep in mind are:

1. $X_1(5)/\mathbf{Z}[1/5]$ is proper and smooth with connected geometric fibers.
2. The locus in $X_1(5)$ over which the fibers of the universal family are not smooth is a relative Cartier divisor and is (finite) étale over $\mathbf{Z}[1/5]$. This divisor is called the *cuspidal locus.*
3. The complement of the cuspidal locus is $Y_1(5)$.
4. The cuspidal locus is a disjoint union of two packets of cusps. In one packet, all the cusps (i.e. sections of the cuspidal locus) are defined over $\mathbf{Z}[1/5]$; in the other packet, the sections are defined over the degree-2 (where $2 = (5-1)/2$) étale cover $\mathrm{Spec}(\mathbf{Z}[1/5, T]/(T^2 - 11T - 1) = \mathrm{Spec}(\mathbf{Z}[1/5, (1 + \sqrt{5})/2]$. Note here that

$\mathbf{Q}((1+\sqrt{5})/2)$ is the maximal totally real subfield of $\mathbf{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity. The first packet parameterizes 5-gons and the second parameterizes 1-gons.

The first three properties are common to all $X_1(N)$ (for $N \geq 5$), and the division of cusps into two packets holds for $X_1(N)$ with $N \geq 5$ prime. (The division into packets is slightly more complicated for composite N: there is one packet for each positive divisor d of N, and it contains $\phi(d)\phi(N/d)/2$ cusps, i.e. each geometric fiber over $\mathrm{Spec}(\mathbf{Z}[1/N])$ contains $\phi(d)\phi(N/d)/2$ points.)

Finally, note that the case of $N = 4$ differs from the $N = 5$ case. The reader should analyze the degenerations of the the universal curve over $Y_1(4)/\mathbf{Q}$ to see that the analogue of Proposition 4.1 does not hold. In fact, the moduli problem of [DR73] for compactifying $Y_1(4)$ is not representable; automorphisms (or rather the twists derived from them) provide an obstruction as in the case of $Y_1(1)$ discussed in §3.

5. The compactifications $X_1(N)$ in general

For a thorough discussion of the moduli problem used to describe $X_1(N)/\mathbf{Z}[1/N]$, one should consult [DR73]. One considers objects E/S of the following sort, called *generalized elliptic curves*:

1. E/S is proper, finitely presented, and flat with connected (but perhaps not smooth and not irreducible) geometric fibers.
2. The geometric fibers of E/S are either smooth genus-1 curves or d-gons.
3. The scheme E^{sm}/S is given the structure of a group scheme.
4. There is an action $E^{\mathrm{sm}} \times E \to E$ extending the group multiplication on E^{sm}.
5. This multiplication action induces cyclic permutations (rotations) on the irreducible components of d-gon geometric fibers.

For the level structure, one considers pairs $(E/S, P)$ of a generalized elliptic curve E/S and a section $P \in E^{\mathrm{sm}}(S)$ such that in each geometric fiber, P has exact order N and the multiples of P meet each connected component. These conditions on P imply that the d-gon fibers of E/S must have $d|N$. Another useful way to describe a section P satisfying the conditions is to give a closed immersion (and group-scheme homomorphism) $\underline{\mathbf{Z}/N\mathbf{Z}} \to E^{sm}/S$ so that the underlying closed subscheme is an S-ample relative Cartier divisor on E.

The functor H_N : (Schemes/$\mathbf{Z}$[1/N]) $\to$ (Sets) of isomorphism classes of such pairs (E, P) is represented by a proper, smooth curve $X_1(N)/\mathbf{Z}[1/N]$. The smoothness is checked using the functorial criterion and the deformation theory of generalized elliptic curves; related considerations allow one to compute the tangent spaces of the geometric fibers. Properness (checked using the valuative criterion) is a consequence of the stable reduction theorem for elliptic curves and a bit of work with minimal regular models of elliptic curves over discretely valued fields.

The locus of non-smooth fibers for the universal family is a relative Cartier divisor in $X_1(N)$ over $\mathbf{Z}[1/N]$ and is called the *cuspidal locus*. It is finite étale over $\mathbf{Z}[1/N]$ and is denoted $\mathrm{Cusps}_1(N)$. The complement of the cuspidal locus is the open subscheme $Y_1(N)$. Using the transcendental uniformization of $Y_1(N)(\mathbf{C})$ (and the Stein factorization of $X_1(N)/\mathbf{Z}[1/N]$), one sees that the geometric fibers of $X_1(N)/\mathbf{Z}[1/N]$ are connected.

For N prime, $\mathrm{Cusps}_1(N)/\mathbf{Z}[1/N]$ behaves as in the $N = 5$ case above. There are two packets of cusps, corresponding to the 1-gon and N-gon degenerations. Since $\mathrm{Cusps}_1(N)/\mathbf{Z}[1/N]$ is étale, to describe the structure of this scheme, it suffices to describe the Galois set $\mathrm{Cusps}_1(N)(\overline{\mathbf{Q}})$. This set has $N-1$ elements, split into the two (Galois-stable) packets of size $(N-1)/2$. The Galois action on the N-gon packet is trivial, i.e. the N-gon cusps are defined over $\mathbf{Q}$. The group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts transitively on the points of the 1-gon packet; this action factors through $\mathrm{Gal}(\mathbf{Q}(\zeta_N)^+/\mathbf{Q})$, where $\mathbf{Q}(\zeta_N)^+$ is the maximal totally real subfield of the N^{th} cyclotomic field. The reader should check this description by computing the isomorphism classes of d-gons with N-level structure (over $\overline{\mathbf{Q}}$) that occur in the moduli problem above, along with the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on these isomorphism classes. (It may help to look at the first few sections of [DR73].) For $N > 5$ that is not prime, the cusps fall into packets parameterizing d-gons for each positive $d|N$.

The reader should also consider the moduli problem above for $X_1(4)$ and see how an extra automorphism (and hence twists) provides an obstruction for representability. (The problem occurs with 2-gons and explains the type of the degeneration of $E(T,0)$ over $Y_1(4)$ at $1/T = 0$.)

Exactly as in the $N = 5$ case, one deduces the following:

Proposition 5.1. *Let $N \geq 5$ be an integer and let R be a discrete valuation ring with residue characteristic not dividing N. Let K be the quotient field of R and E/K be an elliptic curve. Suppose there is a point $P \in E(K)$ of exact order N. Then E/K has stable—i.e. good or multiplicative— reduction.*

As noted above, the proposition fails for $N = 4$: although an E/K with a rational 4-torsion point and potentially good reduction must have good reduction, there are such curves with potentially multiplicative but unstable reduction (and the degeneration of $E(T,0)$ at $1/T = 0$ provides an example).

5.1. **What happens to $X_1(N)$ at primes dividing N.** In the above discussion, the behavior of $X_1(N)$ over $\mathbf{Z}[1/N]$ has been considered. I do not want to address in detail what happens over primes dividing N, but it may be valuable for the reader to have a sense of the new phenomena, as they are important in [Maz77] and many other places. Consider a pair (E,P) consisting of an elliptic curve over a number field K with a point P of exact order N. For a finite place v of K prime to N, if E has good reduction modulo v, then P extends to a section of exact order N of $E/\mathcal{O}_v$. The situation for other v is different in that there are two ways (E,P) can degenerate: either E can have bad reduction at v or, if E has good reduction and $v|N$ then P can have bad reduction, in that the reduction of P in $E(k_v)$ does not have exact order N. This second sort of degeneration certainly occurs if E has supersingular reduction at v.

The model of $Y_1(N)$ over $\mathbf{Z}$ obtained from Tate normal form as in §§1-2 excludes both of these sorts of degenerations in the fibers over primes p dividing N. Consequently, the map of this model to $\mathbf{A}^1$ given by the j-invariant is not finite, since the fibers over the supersingular points are empty. (In the concrete case of $N = 5$, the reader will observe that if K is a field of characteristic 5 then none of the curves $E(b,b)$ with $\Delta(b,b) \in K^\times$ is supersingular.) It is a delicate matter to find a moduli problem extending the elliptic-curve-with-section-of-exact-order-N problem that defines, say, a curve $Y_1(N)/\mathbf{Z}$ finite over the j-line. The reader can find the appropriate problem in [KM85]. One should note that in characteristic dividing N, the Tate-normal-form model of $Y_1(N)$ is missing entire irreducible components of the (correct) Katz-Mazur model of $Y_1(N)$. These missing components may also be non-reduced. For instance, if N is prime, there are two components: a dense open in one is provided by the Tate-normal-form model, and the other is non-reduced with multiplicity $(N-1)/2$; these two components cross at the supersingular points. In terms of degenerations, the points of the non-reduced component come by reduction of pairs (E,P) where E has good reduction and P reduces to the identity. Keeping the assumption that N is prime, one find that (the Katz-Mazur model of) $Y_0(N)$ has two reduced components in its modulo-N fiber. These components are rational curves and cross each other at supersingular points. In both cases, the schemes are regular away from the supersingular crossing points, and the singularities at these crossing points can be analyzed explicitly (with considerable effort, if one wants to find the minimal regular model).

Non-smooth fibers are a general phenomenon among modular curves over $\mathbf{Z}$. Without worrying about the precise structures mentioned in the previous paragraph, one can get a sense for this as follows: for simplicity, let $N = p \geq 5$ be a prime. Suppose that there is a proper flat model $X_1(p)/\mathbf{Z}_p$ that is modular in the sense that the j-invariant map extends to $j : X_1(p) \to \mathbf{P}^1$ over $\mathbf{Z}_p$. Then any point in the special (geometric) fiber of $X_1(p)$ with supersingular j-invariant must be a singular point of this fiber. Indeed, if not, then by Hensel's lemma such a point would lift to a section of $X_1(p)$ over $\mathcal{O}_K$, where $K/\mathbf{Q}_p$ is unramified, i.e. there would be an elliptic curve E/K with supersingular reduction and a K-point of exact order p. In particular, the action of $\mathrm{Gal}(\overline{K}/K)$ on the p-torsion would be reducible, but this is impossible since it is known that in this situation $(e < p-1)$, the inertia group acts irreducibly on the p-torsion. (This fact is proved in [Ser72] and also follows from the more general [Ray74].) Note, incidentally, that $X_1(5)/\mathbf{Z}[1/5]$ does extend to a smooth scheme over $\mathbf{Z}$ (viz $\mathbf{P}^1/\mathbf{Z}$), but that this extension cannot be modular in the sense indicated above.

6. Modular correspondences

In the Mazur-style theory of modular curves, there are three principal sorts of modular correspondences: diamond operators, Atkin-Lehner involutions, and Hecke correspondences. (The Atkin-Lehner involutions are also often called Fricke involutions.) Having the modular curves $Y_1(N)/\mathbf{Z}[1/N]$ and $X_1(N)/\mathbf{Z}[1/N]$, one has two choices of how to handle them. One can define all of the correspondences directly over $\mathbf{Z}[1/N]$, which requires a bit of care, or one can define things, say, over $\mathbf{Q}$ and extend to $\mathbf{Z}[1/N]$ as needed using, for instance, the Néron mapping property. The first approach is more satisfying, but the second has the advantage that one may generally work with $Y_1(N)/\mathbf{Q}$ in place of $X_1(N)$. For instance, to define an automorphism of $X_1(N)/\mathbf{Q}$, it suffices to give an automorphism of its function field (or of $Y_1(N)/\mathbf{Q}$, which ensures the automorphism preserves the cuspidal divisor). I will follow this easy birational approach, inviting the reader to look up or think out how to handle things working directly over $\mathbf{Z}[1/N]$. (One can use a similar birational approach, but the schemes involved are 2-dimensional instead of 1-dimensional, necessitating more care.)

6.1. **Diamond operators.** The diamond operators are the easiest to define: let $N \geq 4$ be an integer. For any $a \in (\mathbf{Z}/N\mathbf{Z})^\times$, one has an automorphism $\langle a\rangle$ of $Y_1(N)/\mathbf{Z}[1/N]$; on S-points for any $S/\mathbf{Z}[1/N]$, the automorphism $\langle a\rangle$ acts by sending (E,P) to $(E,[a]P)$. For $N \geq 5$, the moduli problem of [DR73] allows one to extend this modular definition to give an automorphism of $X_1(N)$. Note that $\langle -1\rangle$ acts trivially since (E,P) is isomorphic to $(E,[-1]P)$ by multiplication by -1. (The automorphism $[-1]$ extends to the generalized elliptic curves E/S used in the moduli problem defining $X_1(N)$.) One must remember, though, that in the theory of modular forms, the operator $\langle -1\rangle$ does not act trivially. Since a generic elliptic curve (what do I mean by that?) has no automorphisms other than $[1]$ and $[-1]$, the diamond operators act faithfully through the quotient $(\mathbf{Z}/N\mathbf{Z})^\times/\pm 1$ on $X_1(N)/\mathbf{Z}[1/N]$.

Note finally that since the diamond operators have a modular definition on all of $X_1(N)$, they preserve the grouping of cusps into packets of d-gons described above. If N is prime, by looking at the modular description of the cusps, one sees furthermore that cusps in each packet are permuted transitively by the diamond operators.

As an example, one can check using the multiplication formulas in §1 that in the $N=5$ case (when there is only one non-trivial diamond operator) that $\langle -2\rangle$ acts by $T \mapsto -1/T$ on $Y_1(5)$ with the coordinate T used above. Note that, in accordance with the general picture, this action switches the two cusps 0 and ∞, which make up the 5-gon packet, and it switches the two 1-gon cusps, whose locus is $T^2-11T-1=0$.

6.2. **Atkin-Lehner involutions.** Let T be a $\mathbf{Z}[1/N]$-scheme and $\zeta \in \Gamma(T,\mathcal{O}_T)$ a primitive N^{th} root of unity. Associated to ζ, there is an involution w_ζ of $Y_1(N)/T$ that is defined as follows. On S-points for S a T-scheme, this involution acts by sending (E,P) to $(E/\langle P\rangle, P' \bmod \langle P\rangle)$, where P' is an N-torsion section of E such that $(P,P')_N = \zeta$ and where $(\cdot,\cdot)_N$ denotes the Weil pairing on $E[N]$. One can make the choice of P' over an étale cover of S, and the image of P' in $E/\langle P\rangle$ is defined over S and independent of the choice. Let us note that over $\mathbf{C}$, with a suitable choice of $\zeta \in \mathbf{C}$ depending on one's favored normalizations, the action of w_ζ is induced by $\tau \mapsto -1/N\tau$ on $\mathbf{H}$ under the uniformization of $Y_1(N)(\mathbf{C})$.

This modular construction cannot be extended to $X_1(N)$. Taking $T = \operatorname{Spec}(\mathbf{Q}(\zeta_N))$, though, one gets an automorphism of the function field of $X_1(N)/T$ that fixes $Y_1(N)/T$. Consequently, one finds an automorphism of $X_1(N)/\mathbf{Q}(\zeta_N)$ that stabilizes (but may not—and does not—fix pointwise) the cuspidal divisor. One can also make a slightly fancier birational argument in the universal case $T = \mathbf{Z}[1/N,\zeta_N]$ to see that w_ζ extends to an automorphism of $X_1(N)/\mathbf{Z}[1/N,\zeta_N]$.

From the modular definition, one finds the following functional equations

$$\begin{aligned} w_\zeta \circ \langle a\rangle &= \langle a^{-1}\rangle\, w_\zeta \\ w_{\zeta^a} \circ w_\zeta &= \langle a\rangle\,. \end{aligned}$$

As a consequence of these relations one sees that the group of automorphisms of $X_1(N)/T$ generated by the diamond operators and Atkin-Lehner involutions is a split extension of $\mathbf{Z}/2\mathbf{Z}$ by the group of diamond operators, where the action of $\mathbf{Z}/2\mathbf{Z}$ on the normal subgroup is by $x \mapsto x^{-1}$.

The action of an Atkin-Lehner involution w_ζ on the cusps is more complicated than the action of the diamond operators since there is no modular definition outside of $Y_1(N)$. It can be computed using degenerating families near each cusp; the Tate curve (which is not discussed here) provides particularly nice choices of families for such computations (but any family degenerating to a cusp will do). In particular, one can show that for N prime, an operator w_ζ switches the 1-gon and N-gon packets of cusps, as the reader should check. (For N not prime, one ought to define more Atkin-Lehner involutions, one for each square-free divisor of N. The group generated by all of these extra Atkin-Lehner involutions and the diamond operators acts transitively on the cusps precisely when N is square free.)

6.3. **Hecke correspondences.** The Hecke correspondences are the geometric manifestations of the Hecke operators. The classical theory of Hecke correspondences goes back to Fricke and Klein (making it odd perhaps for me to call them Hecke correspondences). A fairly complete discussion of their formalism can be found in Chapter 7 of [Shi94], among other places.

Recall that an isogeny $\phi : E \to E'$ of elliptic curves over a scheme S is a faithfully flat (finite) homomorphism of S-group schemes. The standard example of an isogeny is the map $[n] : E \to E'$ for any integer $n \neq 0$. (Why is this map an isogeny?) The group scheme $\ker(\phi)$ is finite and flat over S. Its rank, a locally constant function on S, is called the *degree* of the isogeny; if the rank is a constant n, then ϕ is said to be an *n-isogeny*. If (E, P) and (E', P') are pairs of an elliptic curve and section over a base S, an *isogeny* $\phi : (E, P) \to (E', P')$ is an isogeny $\phi : E \to E'$ such that $\phi(P) = P'$. There is an evident notion of isomorphy between such structures ϕ.

Let $n \geq 1$ be an integer and fix $N \geq 4$. The *Hecke correspondence of level n* (for $Y_1(N)$) is a scheme $\mathrm{Isog}_n / \mathbf{Z}[1/Nn]$ whose S-points are the isomorphism classes of isogenies $\phi : (E, P) \to (E', P')$ over S of constant degree n. There are two projections $\pi_1, \pi_2 : \mathrm{Isog}_n \to Y_1(N)$ over $\mathbf{Z}[1/Nn]$, defined on S-points as the source and target of the n-isogeny, respectively.

I will not prove the existence of the scheme Isog_n for general n but will restrict myself to $n = p$, a prime number. The construction comes in two steps. First, let (E^u, P^u) be the universal pair over $Y_1(N)/\mathbf{Z}[1/Np]$. Consider the scheme $E^u[p]$, which is a finite étale cover of $Y_1(N)$. The S-points of $E^u[p]$ parameterize isomorphism classes of triples (E, P_N, P_p), where E/S is an elliptic curve, P_N is a section of exact order N, and P_p is a p-torsion section. If $(p, N) = 1$, let Z be open subscheme of $E^u[p]$ obtained by removing the zero section; if $p|N$, let Z be the complement in $E^u[p]$ of the sections $[aN/p]P^u$ for all integers a. Then the S-points of Z parameterize isomorphism classes of triples (E, P_N, P_p), where E/S is an elliptic curve, P_N is a section of exact order N, and P_p is a section of exact order p that is not a multiple of P_N in any geometric fiber.

One can equally well describe the structures parameterized by Z by giving data

$$(\phi : (E, P_N) \to (E', P'_N), \psi : \underline{\mathbf{Z}/p\mathbf{Z}} \to \ker(\phi)),$$

where E, E' are elliptic curves over S with sections P, P' of exact order N; ϕ is an isogeny from (E, P_N) to (E', P'_N); and ψ is an isomorphism from $\underline{\mathbf{Z}/p\mathbf{Z}}$ to $\ker(\phi)$. To translate between the two pictures, take $E' = E/\langle P_p \rangle$, $P'_N = P_N \bmod P_p$, and $\psi(1) = P_p$. From this point of view, Z is quite close to the desired Isog_p, but it carries the extra information of ψ.

The second step in the construction is to remove the extra data of ψ. To this end, we consider an action of $G = (\mathbf{Z}/p\mathbf{Z})^\times$ on Z that is quite similar to the diamond operators defined above. Namely, for $a \in (\mathbf{Z}/p\mathbf{Z})^\times$, define $\langle a \rangle$ acting on Z by the rule $(\phi, \psi) \mapsto (\phi, a\psi)$ on S-points. This action is free in the sense that its graph $G \times Z \to Z \times Z$ (products over $\mathbf{Z}[1/Np]$) is a closed immersion. To get Isog_p, one forms the quotient of Z by the action of G. One can find the general properties of free quotients in [Ray67], from which it follows that this quotient is the desired Isog_p.

Note that as with the Atkin-Lehner involutions, there is no direct modular construction of the compactified Hecke correspondences Isog_n over $X_1(N)$. One can produce such a compactification over $\mathbf{Q}$ as before by considering function fields. The behavior over the cusps can be determined using degenerating families and (when expressed in terms of the Tate curve) is related to the classical formulas for the action of Hecke operators on q-expansions.

The geometric theory of these Hecke correspondences can be carried several steps further. For example, the composition of isogenies yields

$$\mathrm{Isog}_n \times_{Y_1(N)} \mathrm{Isog}_m \to \mathrm{Isog}_{nm},$$

since degree of isogenies is multiplicative under composition. Naturally, the product is taken over the source arrow in the first factor and the target arrow in the second factor. These product structures are then related to the composition of Hecke operators.

Another important development of this geometric theory is the study of $\mathrm{Isog}_p / Y_1(N)$ over $\mathbf{Z}[1/N]$ (in place of $\mathbf{Z}[1/Np]$). The above construction of Isog_p no longer applies, since the kernel of a p-isogeny over a field of characteristic p need not be étale. A slightly fancier argument along the same lines does still produce Isog_p. It is often sufficient to study the simpler subscheme parameterizing p-isogenies $\phi : (E, P_N) \to (E', P'_N)$ over $\mathbf{Z}[1/N]$-schemes such that the characteristic-p geometric fibers of E and E' are ordinary elliptic curves; this scheme Isog^0_p is the *scheme of ordinary p-isogenies.* The map $\mathrm{Isog}^0_p \to \mathrm{Isog}_p$ is an open immersion with dense image in all geometric fibers over $\mathbf{Z}[1/N]$. (Prove this fact.) For a p-isogeny $\phi : E \to E'$ of ordinary elliptic curves over a separably closed field, $\ker(\phi)$ is either isomorphic to $\underline{\mathbf{Z}/p\mathbf{Z}}$ or μ_p; in the second case, ϕ is isomorphic to the Frobenius isogeny of E, and in the first case, its dual $\phi^\vee$ is isomorphic to the Frobenius isogeny. As a consequence of this dichotomy, $\mathrm{Isog}^0_p / \mathbf{F}_p$ is the disjoint union of the open subschemes parameterizing these two types of p-isogenies. (If $\phi : (E, P) \to (E', P')$ is a p-isogeny over a scheme S, then the locus in S over which the finite, flat $\ker(\phi)$ is étale is open. If p is locally nilpotent on S, then the open loci where $\ker(\phi)$ and its Cartier dual, $\ker(\phi^\vee)$, are étale are disjoint; in the ordinary case, the union of these loci is S.) The μ_p locus projects isomorphically onto $Y_1(N)/\mathbf{F}_p$ via its source arrow, and, dually, the $\underline{\mathbf{Z}/p\mathbf{Z}}$ locus projects isomorphically onto $Y_1(N)/\mathbf{F}_p$ via the target morphism. The other two morphisms are finite flat of degree p. This picture of the structure of Isog^0_p is known as the Kronecker (or Eichler-Shimura) congruence relation. (The geometric description is due to Shimura.) One should contrast the decomposition of $\mathrm{Isog}_p / \mathbf{F}_p$ into two irreducible components with the irreducibility of $\mathrm{Isog}_p / \mathbf{C}$.

6.4. **Action on modular forms.** The above three types of modular correspondences all can be viewed in the form (say over $K = \mathbf{Q}$ or $\mathbf{Q}(\zeta_N)$ for the Atkin-Lehner involutions) of a pair of finite (flat) maps $\pi_1, \pi_2 : M \to X$ where X is a proper modular curve and M is another (not necessarily geometrically connected) curve over K. In the first two cases, M is simply the graph of a diamond-operator automorphism or of an Atkin-Lehner involution, and in the third case, M is the scheme Isog_n.

Given such a set-up, or more generally a pair of finite maps $\pi_1 : M \to X_1$, $\pi_2 : M \to X_2$ with M, X_1, X_2 curves over a field, one can construct a maps $H^1(X_2) \to H^1(X_1)$ and $H_1(X_1) \to H_1(X_2)$, where H^1 is any reasonable functor that behaves like a degree-1 cohomology and H_1 is any reasonable functor that behaves like a degree-1 homology. The simplest case is when M is the graph of a morphism $X_1 \to X_2$, in which case the maps just come from the functoriality. More generally, to produce $H^1(X_2) \to H^1(X_1)$, one composes the pullback map $H^1(X_2) \to H^1(M)$ with a trace map $H^1(M) \to H^1(X_1)$. (The existence of such a trace map is implicit in the requirement that the functors be "reasonable.")

The universal construction of this sort is $\mathrm{Jac}(X)$, the Jacobian of X. Classically, the Jacobian has a dual nature: it can viewed contravariantly (as classifying line bundles) or covariantly (as classifying cycles of degree 0). The contravariant functoriality is often called (by number theorists, at least) *Picard functoriality* and the covariant functoriality is often called *Albanese functoriality.* When viewed contravariantly, $\mathrm{Jac}(X)$ should be considered as a manifestation of $H^1(X)$ (or really of $H^1(X, \mathbf{Z}(1))$), and when viewed covariantly, of $H_1(X, \mathbf{Z})$. To keep these two functorialities straight, one typically uses a notation $(\cdot)_*$ for Albanese (homological) and $(\cdot)^*$ for Picard (cohomological). In [Maz78], Mazur generally considers the Albanese functoriality, thinking of Jacobians as homology. With this picture in mind, we obtain from the modular correspondences above automorphisms $\langle a \rangle_*$ of $J_1(N)/\mathbf{Q}$ from the diamond operators, automorphisms $(w_\zeta)_*$ of $J_1(N)/\mathbf{Q}(\zeta_N)$ from the Atkin-Lehner involutions, and endomorphisms $(T_n)_* : J_1(N) \to J_1(N)$ over $\mathbf{Q}$ from the Hecke correspondences Isog_n. The notation $J_1(N)$ is standard shorthand for $\mathrm{Jac}(X_1(N))$, and in general one indicates Jacobians of proper modular curves by replacing the X in the notation with a J.

Although it is not a complete cohomology theory, the space of 1-forms of the first kind satisfies the necessary formalism to construct a cohomological functoriality of the sort described above:

1. One has automorphisms of $H^0(X_1(N)/\mathbf{Q}, \Omega^1_{X_1(N)/\mathbf{Q}})$ coming from the diamond operators,
2. automorphisms of $H^0(X_1(N)/\mathbf{Q}(\zeta_N), \Omega^1_{X_1(N)/\mathbf{Q}(\zeta_N)})$ coming from the Atkin-Lehner involutions,
3. and endomorphisms T_n^* of $H^0(X_1(N)/\mathbf{Q}, \Omega^1_{X_1(N)/\mathbf{Q}})$ coming from the Hecke correspondences.

Working over $\mathbf{C}$, the space $H^0(X_1(N)/\mathbf{C}, \Omega^1_{X_1(N)/\mathbf{C}})$ can be identified with the weight-2 cusp forms on $\Gamma_1(N)$. (Keep in mind that holomorphic and algebraic 1-forms of the first kind on a proper smooth curve over $\mathbf{C}$ are the same thing. This can be seen in various fairly elementary ways, or, to use a sledgehammer, simply by invoking Serre's GAGA.) In fact, these geometrically defined endomorphisms of the weight-2 cusp forms (with a suitable choice of N^{th} root of unity in $\mathbf{C}$ for the Atkin-Lehner involutions) agree with the classical operators described in [Shi94].

Note that the 1-forms of the first kind on $X_1(N)$ can be recovered from $J_1(N)$ by the classical identification of invariant differentials on $\mathrm{Jac}(X)$ with the 1-forms on the first kind on X. Furthermore if we use this identification to define endomorphisms of $H^0(X_1(N)/K, \Omega^1_{X_1(N)/K})$ by functoriality from the (Albanese) endomorphisms $(T_n)_*$ (etc.) of $\mathrm{Jac}(X_1(N))$, we get the same endomorphisms as in the direct definition immediately above.

7. The curves $Y_0(N)$ and $X_0(N)$

In addition to the curves $Y_1(N)$ and $X_1(N)$ discussed above, it is useful to have arithmetic models of the curves $Y_0(N)$ and $X_0(N)$.

7.1. **Coarse moduli spaces and** $Y_0(N)$**.**

One might hope to define the curve $Y_0(N)/\mathbf{Z}[1/N]$ as a scheme representing the functor whose S-points classify pairs (E, C), where E/S is an elliptic curve and C is a cyclic subgroup of E/S of order N; this second condition should be taken to mean that C/S is a finite, flat subgroup scheme of E/S and that étale locally on S, the group scheme C is isomorphic to $\underline{\mathbf{Z}/N\mathbf{Z}}$. For instance, if $S = \mathrm{Spec}(K)$ for a field K with a separable closure K_s, then to give such a C/S is equivalent to giving a $\mathrm{Gal}(K_s/K)$-stable subgroup of $E[N](K_s)$ that is cyclic of order N. Unfortunately, this functor is not representable: the problem is that any such pair (E, C) has an automorphism, namely $[-1]$; the presence of this automorphism allows one to construct twists, which provides an obstruction to representability. Instead, we define $Y_0(N)$ to be the quotient of $Y_1(N)/\mathbf{Z}[1/N]$ by the group G of diamond operators. Recall the universal mapping property of quotients: if G acts on X, then we say that $X \to X'$ is a quotient of X by G if for any morphism $f : X \to T$ that is invariant under G, we have a unique factorization $X \to X' \to T$ of f through X'. Evidently such a quotient X' is determined up to unique isomorphism compatible with $X \to X'$.

Even though $Y_0(N)$ and $X_0(N)$ are not moduli schemes classifying pairs (E, C) as above, they are quite closely related to this moduli problem. Let us consider only $Y_0(N)$—everything carries through to $X_0(N)$ if one considers generalized elliptic curves as in [DR73]. Before discussing $Y_0(N)$ in particular, we consider a few more issues related to representability of functors. Let $F : (\text{Schemes/T}) \to (\text{Sets})$ be a functor. Recall that a pair (Y, i) of a T-scheme Y and a natural transformation $i : F \Rightarrow Y$ is said to represent F if for each T-scheme S, the map $i : F(S) \to Y(S)$ is a bijection. (In §2 the natural transformation i would have been denoted i^{-1}. This should not cause much confusion; it should also be evident that there is some justification for the switch in notation.) To understand $Y_0(N)$, we consider the following pair of weaker conditions:

1. For $S = \mathrm{Spec}(k)$ with k an algebraically closed field, $i : F(S) \to Y(S)$ is a bijection.
2. For any scheme Y' and natural transformation $i' : F \Rightarrow Y'$, there is a unique morphism $f : Y \to Y'$ such that $f \circ i = i'$. Informally, Y is the closest approximation to F in the category of schemes over T.

If (Y, i) satisfies these two conditions we say (in non-standard terminology) that Y *coarsely represents* F; if F is a moduli functor for some structure, then we say that (Y, i) is a *coarse moduli scheme* for that structure. Evidently (by the second condition) such a coarse moduli scheme (Y, i) is determined up to unique isomorphism compatible with i. One must be more careful with coarse moduli schemes than with schemes actually representing moduli functors (called *fine moduli schemes*): for instance, it is obvious that if (Y, i)

represents a functor F on S-schemes, then for any $S' \to S$, the pair $(Y \times_S S', i)$ represents F restricted to S'-schemes, but the analogous property does not generally hold for coarse moduli schemes; to put it in a phrase "formation of coarse moduli schemes does not generally commute with base change."

The scheme $Y_0(N)/\mathbf{Z}[1/N]$ can be viewed as a coarse moduli space for the problem of classifying pairs (E, C), where E/S is an elliptic curve and C is a cyclic subgroup scheme of order N. To make sense of this, it is first necessary to construct a natural transformation $i : F \Rightarrow Y_0(N)$, where F is the functor whose S-points are isomorphism classes of such pairs. Given (E, C), for any étale S'/S and isomorphism $\psi : \underline{\mathbf{Z}/N\mathbf{Z}} \to C/S'$, one gets an S'-valued point of $Y_1(N)$ and hence of $Y_0(N)$ via the quotient map. For any two choices ψ, ψ' of isomorphism of S', there is finite Zariski-open cover (U_i) of S' such that $\psi = [a] \circ \psi'$ for some $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ on each U_i. Consequently, the S'-point of $Y_0(N)$ is independent of the choice of ψ. Therefore, by étale descent, the collection of S'-points $Y_0(N)$ associated to (E, C) over S comes from a (unique) S-point. (By definition of "cyclic subgroup scheme" collection of such S' is an étale cover of S.) The reader can check that this construction provides a natural transformation $i : F \Rightarrow Y_0(N)$. To check that $(Y_0(N), i)$ is a coarse moduli scheme, the conditions 1. and 2. above must be verified.

The first condition is a general property of quotients (of quasi-projective schemes) by finite groups: one knows that for k an algebraically closed field, $Y_0(N)(k) = (G\backslash Y_1(N))(k) = G\backslash(Y_1(N)(k))$, where G is the group of diamond operators. Evidently $G\backslash(Y_1(N)(k))$ is $F(\operatorname{Spec}(k))$. To check the second condition, suppose we are given a scheme $Y'/\mathbf{Z}[1/N]$ and a natural transformation $i' : F \Rightarrow Y'$. There is an evident natural transformation $Y_1(N) \Rightarrow F$, and so we have a morphism $Y_1(N) \to Y'$. Looking at S-points for all $\mathbf{Z}[1/N]$-schemes S, it is clear that this morphism is invariant under the action of group G of diamond operators; hence it factors uniquely as $Y_1(N) \to G\backslash Y_1(N) = Y_0(N) \to Y'$. A review of how $i : F \Rightarrow Y_0(N)$ was defined shows that this factorization transforms i into i', as required. Evidently there is a general principle lurking behind this discussion, which we will not investigate further; it may be helpful to note, though, that if G acts on a scheme X and the quotient $S = G\backslash Y$ exists, then S coarsely represents the functor $G\backslash \operatorname{Hom}(\cdot, Y)$.

It is sometimes helpful to reinterpret $F(S)$ as the isomorphism classes of cyclic N-isogenies $E \to E'$ of elliptic curves over S. One is thus inclined to view $Y_0(N)$ as (a piece of) the Hecke correspondence of level N over $Y_1(1) \times Y_1(1)$, but in the present discussion such structures have been excluded. As with $Y_0(N)$, one can interpret $Y_1(N)$ with $N = 1, 2, 3$ as a coarse moduli space, which gives solid sense to this inclination.

7.2. Properties of $Y_0(N)/\mathbf{Z}[1/N]$ and $X_0(N)/\mathbf{Z}[1/N]$.

In the appendix of [KM85], the authors prove that for a smooth $Y/\mathbf{Z}[1/N]$ of pure relative dimension 1, the quotient by the action of a finite group is again smooth over $\mathbf{Z}[1/N]$. Consequently, $X_0(N)/\mathbf{Z}[1/N]$ and $Y_0(N)/\mathbf{Z}[1/N]$ are smooth curves (with connected geometric fibers); furthermore, $X_0(N)/\mathbf{Z}[1/N]$ is proper and $Y_0(N)$ is an (affine) open in $X_0(N)$. As with $Y_1(N)$, one can show that $Y_0(N)(\mathbf{C})$ with its structure of a complex manifold is $\Gamma_0(N)\backslash\mathbf{H}$. The complement of $Y_0(N)$ in $X_0(N)$ is a relative Cartier divisor over $\mathbf{Z}[1/N]$, which is étale. It is called the *cuspidal locus*.

From the discussion of the previous section, we see that $Y_0(N)(\overline{\mathbf{Q}})$ is the set of isomorphism classes of (E, C), where $E/\overline{\mathbf{Q}}$ is an elliptic curve and $C \subset E(\overline{\mathbf{Q}})$ is a cyclic subgroup of order N; the same is true for $X_0(N)(\overline{\mathbf{Q}})$ with the appropriate generalized moduli problem. Consequently, the set $Y_0(N)(\mathbf{Q})$, which is the Galois invariants of $Y_0(N)(\overline{\mathbf{Q}})$, has an interpretation in terms of elliptic curves. Keep in mind that $F(\mathbf{Q}) \to Y_0(N)(\mathbf{Q})$ is not injective: two pairs (E, C) and (E', C') in $F(\mathbf{Q})$ define the same point in $Y_0(N)(\mathbf{Q})$ if and only if they are isomorphic over $\overline{\mathbf{Q}}$, i.e. if they are twists of each other.

One might ask, on the other hand, whether $F(\mathbf{Q}) \to Y_0(N)(\mathbf{Q})$ is surjective, i.e. whether each point in $Y_0(N)(\mathbf{Q})$ is represented by a pair (E, C) of an elliptic curve $E/\mathbf{Q}$ and a cyclic subgroup $C \subset E(\overline{\mathbf{Q}})$ that is Galois stable. This is, in fact, true and proved in [DR73] IV-3 by a Galois-cohomology computation. The same result holds for K-points, where K is any field of characteristic prime to N. Along these lines, it may be helpful to consider $Y_0(N)(K)$, where K is a field of characteristic prime to N, as parameterizing elliptic curves E/K whose modulo-N Galois representation factors through the group of upper triangular matrices. (That statement is a bit sloppy.) Similarly one can consider $Y_1(N)(K)$ as parameterizing E/K whose modulo-N Galois representation factors through upper triangular matrices with 1 in the left corner.

The cusps of $X_0(N)$ and their fields of rationality can be determined by using the description of the cusps of $X_1(N)$ in §5. In particular, if N is prime, there are two cusps, each corresponding to a packet of cusps on $X_1(N)$. Both cusps are rational over $\mathbf{Q}$. The 1-gon cusp is usually denoted ∞ and the N-gon cusp 0, on account of the appearance of these cusps in the $\mathbf{H}$-uniformization of $Y_0(N)(\mathbf{C})$.

7.3. **Modular correspondences.** Naturally, there are no diamond operators acting on $Y_0(N)$ or $X_0(N)$. There is an Atkin-Lehner involution, which can be understood either by viewing $Y_0(N)$ as a coarse moduli scheme or as a quotient of $Y_1(N)$. In the coarse-moduli-scheme picture, for any $\mathbf{Z}[1/N]$-scheme S, we have the involution $w(S) : (E, C) \mapsto (E/C, E[N]/C)$ of the set $F(S)$ considered above. If we consider $F(S)$ to be isomorphism classes of cyclic N-isogenies $\phi : E \to E'$, this involution exchanges ϕ and its dual $\phi^\vee : E' \to E$. The various involutions $w(S)$ are functorial in S and so define a natural isomorphism $w : F \Rightarrow F$. One has, therefore, a second coarse moduli space $(Y_0(N), i \circ w)$ for F and so a unique isomorphism $w : Y_0(N) \to Y_0(N)$ satisfying $w \circ i = i \circ w$. This automorphism is the Atkin-Lehner involution. Alternatively, one can obtain this w by considering the Atkin-Lehner involutions w_ζ on $Y_1(N)$. The commutation relations between these involutions and diamond operators show that these involutions induce a single common involution on $Y_0(N)$, defined over $\mathbf{Q}$ (or $\mathbf{Z}[1/N]$). For our purposes, it suffices to extend w to an automorphism of $X_0(N)/\mathbf{Q}$ stabilizing the cusps, which is effortless since w acts on the function field of $X_0(N)/\mathbf{Q}$ and stabilizes $Y_0(N)$. As in the case of $X_1(N)$, it is possible to analyze the action of w on the cusps; in particular, for N a prime, w switches the cusps 0 and ∞.

As for the Hecke correspondences, one can construct a scheme $\mathrm{Isog}_n /\mathbf{Z}[1/N]$ (indeed, a smooth curve) with two projections to $Y_0(N)$ by taking the quotient of the n-isogeny scheme for $Y_1(N)$ by the natural action of the diamond operators. This quotient scheme can be interpreted as a coarse moduli space; the details are left to the reader. As above, we extend Isog_n to the proper, smooth curve over $\mathbf{Q}$ with the same function field. This curve then admits two (finite) projections to $X_0(N)/\mathbf{Q}$, which allow one to construct the Hecke endomorphism $(T_n)_*$ of $J_0(N)/\mathbf{Q} = \mathrm{Jac}(X_0(N))$.

8. A closer look at $X_0(11)$ and $X_1(11)$

Finally, we can have a bit of fun, working out equations for $X_0(11)$ and $X_1(11)$ and a few properties of these curves and their Jacobians. Everyone should know these two examples well, if for no other reason than that their Jacobians are two of the three elliptic curves over $\mathbf{Q}$ with the smallest possible conductor, $N = 11$. The method is a bit sneaky and does not provide equations for the universal elliptic curve over $X_1(11)$, which one may want. It is possible, of course, to work out the equations using Tate normal form, although the computation is rather involved (cf. [Con95]). To begin with, we have the following:

Proposition 8.1. *Let $E/\mathbf{Q}$ be an elliptic curve with good reduction outside of a single prime p. Suppose that $E(\mathbf{Q})$ contains a point of exact order 5. Then $p = 11$ and $E = E(1, 1) = E(-1, -1)$ or $E = E(11, 11) = E(-1/11, -1/11)$.*

Proof. Let $E/\mathbf{Z}[1/p]$ be the Néron model (=minimal Weierstrass model, if you prefer) of E. Note that by [Sil86] Chapter VII, Theorem 3.4 ("specialization principle"), the point $P \in E(\mathbf{Q})$ reduces to point of exact order 5 in each geometric fiber of $E/\mathbf{Z}[1/p]$. (If we were working with $N = 4$ in place of $N = 5$, there could be trouble here, since the specialization principle does not apply to the 4-torsion). Consequently, $(E/\mathbf{Z}[1/p], P)$ is isomorphic to $(E(b, b), (0, 0))$, for some $b \in \mathbf{Z}[1/p]^\times = \pm p^{\mathbf{Z}}$ such that $\Delta(b, b) = b^5(b^2 - 11b - 1) \in \mathbf{Z}[1/p]^\times$. Note here that we are using the universal property of $(E(b, b), (0, 0))$ over $\mathbf{Z}$ and not just over $\mathbf{Z}[1/5]$.

By replacing P with $2P$, if necessary, we may assume that $b \in \mathbf{Z}$ (and so $\Delta(b, b) \in \mathbf{Z}$). (The diamond operator acts by $b \mapsto -1/b$.) We must have either $b = \pm 1$ or $p|b$. In the first case, we have $E = E(1, 1) = E(-1, -1)$; therefore, $\Delta(b, b) = -11$, and so $p = 11$. In the second case, we have both $b^2 - 11b - 1 \equiv -1 \pmod p$ and $b^2 - 11b - 1 = \pm p^n$ for some $n \geq 0$; and so either $b^2 - 11b - 1 = -1$ (i.e. $b = 11$) or $b^2 - 11b - 1 = 1$ and $p = 2$. There are no roots to $b^2 - 11b - 2 = 0$ in $\mathbf{Z}$, and so we must in fact have $p = 11$ and $E = E(11, 11)$. □

To put this proposition into perspective, note that if $E/\mathbf{Q}$ is an elliptic curve with good reduction at 2, then $E(\mathbf{Q})$ can contain no non-trivial l-torsion for any prime $l > 5$, as follows by applying the Weil bound to the reduction modulo 2. If $E/\mathbf{Q}$ has good reduction outside of 2, then the Weil bounds for the modulo-3 reduction show that E cannot have non-trivial l-torsion for any prime $l > 7$; we saw above that $l = 5$ is impossible, and one can check that $l = 7$ is also impossible. (To check the $l = 7$ case, one can use Tate normal form as in $l = 5$ case—see [Con95], page 278 for the formulas.) In summary, if $E/\mathbf{Q}$ is an elliptic curve with bad reduction at only one place, it can have only non-trivial 2-power, 3-power, or 5-power torsion, and the above proposition describes the 5-power torsion case.

8.1. **Properties of $X_0(11)$ and $X_1(11)$.** Now let us summarize some facts about $X_0(11)/\mathbf{Q}$ and $X_1(11)/\mathbf{Q}$. First, both curves are proper, smooth, connected, and of genus 1 (cf. [Shi94] for genus formulas based on the map to the j-line) and extend to proper, smooth curves over $\mathbf{Z}[1/11]$. All the geometric fibers have genus 1. There is a canonical map $\pi : X_1(11) \to X_0(11)$ (even over $\mathbf{Z}[1/11]$), given by the realization of $X_0(11)$ as the quotient of $X_1(11)$ by the action of the diamond operators. This map is an étale (Galois) covering of degree 5, as follows from the fact that the geometric fibers of $X_1(11)$ and $X_0(11)$ over $\mathbf{Z}[1/11]$ are all of genus 1.

The curve $X_0(11)$ has two cusps, both rational over $\mathbf{Q}$, usually called 0 and ∞, and which correspond to 11-gons and 1-gons, respectively. The curve $X_1(11)$ has two packets of cusps, the five 11-gon cusps in $X_1(11)(\mathbf{Q})$, and the packet of five 1-gon cusps in $X_1(11)(\mathbf{Q}(\zeta_{11})^+)$. These two packets are the fibers of π over 0 and ∞, respectively.

The map π induces a homomorphism $\phi : J_1(11)/\mathbf{Q} \to J_0(11)/\mathbf{Q}$. (Since $X_0(11)$ and $X_1(11)$ are genus-1 curves with rational points, they can be identified with their Jacobians, but it is probably clearer to consider these are distinct objects. To see why, note, for instance, that the diamond operators act trivially on $J_1(11)$.) This map is a degree-5 isogeny, since it comes from the unramified Galois cover π. For any (rational) cusp c in the 11-gon packet of $X_1(11)$, we have $\pi(c) = 0$. Therefore the points $[c'] - [c] \in J_1(11)(\mathbf{Q})$ (where c, c' run over the N-gon cusps of $X_1(11)$) all map to the identity in $J_0(11)(\mathbf{Q})$. Since $X_1(11)$ has genus 1, if we fix one such cusp c_0, the five differences $[c_0] - [c]$ are distinct. We conclude that $\ker(\phi)$ is a constant group scheme over $\mathbf{Q}$ (isomorphic to $\underline{\mathbf{Z}/5\mathbf{Z}}$) and that $\ker(\phi)(\mathbf{Q})$ consists of the points $[c'] - [c]$ where c, c' run over the 11-gon cusps. (The points $[c_0] - [c]$ for a fixed c_0 give a list of these five points without redundancies.)

The Weil pairing on $J_1(11)[5]$ gives an identification of $J_1(11)[5]/\ker(\phi)$ with μ_5. Consequently, we know that $J_0(11)[5]$ contains a subgroup scheme isomorphic to μ_5, viz the image of $J_1(11)[5]$. (If you do not like group schemes, it is quite sufficient to think about Galois modules, since we are working over $\mathbf{Q}$ at this point.) This subgroup scheme is usually called the Shimura subgroup of $J_0(11)$. By general properties of isogenies of elliptic curves, it can also be considered as the kernel of the dual isogeny $\phi^\vee : J_0(11) \to J_1(11)$.

Consider the point $[0] - [\infty] \in J_0(11)(\mathbf{Q})$. One knows from the analytic theory of modular forms (more precisely, from the transformation formulas for Dedekind's η function) that $(\Delta(z)/\Delta(11z))^{1/2}$ is a rational function on $X_0(11)/\mathbf{C}$. Its divisor is $5[0] - 5[\infty]$, and so the point $[0] - [\infty] \in J_0(11)(\mathbf{Q})$ has order dividing 5. It can not be trivial, since $X_0(11)$ does not have genus 0, and so it must have exact order 5. (It is possible to complete this step without invoking such analytic theory, if one develops the algebraic theory of modular forms.) The constant subgroup scheme generated by $[0] - [\infty]$ is usually called the cuspidal subgroup of $J_0(11)$. Together with the Shimura subgroup, it gives a splitting (over $\mathbf{Q}$) $J_0(11)[5] = \underline{\mathbf{Z}/5\mathbf{Z}} \oplus \mu_5$, which can be understood either in terms of group schemes or Galois modules.

We deduce from the proposition that $J_0(11)$ is either $E(1,1)$ or $E(11,11)$ and the same for $J_1(11)$. In fact:

Proposition 8.2. *We have* $J_0(11)/\mathbf{Z}[1/11] = E(11,11) = E(-1/11,-1/11)$ *and* $J_1(11)/\mathbf{Z}[1/11] = E(1,1)$.

Proof. Note that it suffices to check that $J_0(11)/\mathbf{Q} = E(11,11)$ and $J_1(11)/\mathbf{Q} = E(1,1)$, since the models over $\mathbf{Z}[1/11]$ are the Néron models (or minimal Weierstrass models, if you prefer) of the $\mathbf{Q}$-fibers.

Let us see that $J_0(11)$ and $J_1(11)$ are not isomorphic or even twists of each other. If, in fact, the two curves were isomorphic (over any extension of $\mathbf{Q}$), then the degree-5 isogeny $J_1(11) \to J_0(11)$ would exhibit a complex multiplication. Any elliptic curve over $\mathbf{Q}$ with (potential) complex multiplication has potentially good reduction everywhere, but both $E(1,1)$ and $E(11,11)$ have multiplicative reduction at $p = 11$ and so can not have (potential) complex multiplication.

It remains, therefore, to show $J_0(11)/\mathbf{Q} \neq E(1,1)$. Recall that $E(1,1)$ is described by the Weierstrass equation $y^2 - y = x^3 - x^2$. Considering this equation over $\mathbf{Z}_{11}$, one gets a closed subscheme $E(1,1)$ of $\mathbf{P}^2/\mathbf{Z}_{11}$, flat over $\mathbf{Z}_{11}$ and with a section (at infinity) passing through its smooth locus; its generic fiber is an elliptic curve, and the special fiber is a nodal cubic. Note moreover that as an abstract scheme, it is regular, since even at the singular point $(0,0)$ of the special fiber, the defining equation is not in the square of the maximal ideal. Consequently, any section of $E(1,1)$ over $\mathbf{Z}_{11}$ must pass through the smooth locus of the special fiber. Consider, in particular, $E(1,1)[5](\mathbf{Q}_{11}) = E(1,1)^{\mathrm{sm}}[5](\mathbf{Z}_{11})$. Since 5 and 11 are coprime, the reduction map on 5-torsion is injective, and so we get $E(1,1)[5](\mathbf{Q}_{11}) \subset E(1,1)^{\mathrm{sm}}[5](\mathbf{F}_{11})$. The group structure on $E^{sm}/\mathbf{Z}_{11}$ makes the special fiber a torus, so that $\#E(1,1)^{sm}[5](\mathbf{F}_{11}) \leq 5$. On the other hand, $J_0(11)[5](\mathbf{Q}_{11}) = \mathbf{Z}/5\mathbf{Z} \oplus \mu_5(\mathbf{Q}_{11})$, which has order 25, and so $J_0(11)/\mathbf{Q} \neq E(1,1)$. □

From the above identification of $(J_0(11), [0] - [\infty])$ with $(E(11,11),(0,0))$ or $(E(-1/11,-1/11),(0,0))$ (and the analysis of degenerations in §4), we see that the cuspidal subgroup does not reduce to the identity component of the Néron model at 5. In fact, since $\Delta(11,11) = -11^5$, one knows that this fiber of the Néron model has exactly 5 components; the reduction of the cuspidal subgroup gives a splitting of the component group. Going back to $X_0(11)$, one deduces that its minimal regular model over $\mathbf{Z}$ has a 5-gon fiber at $p = 11$.

As for $J_1(11) = E(1,1)$, we see that all the fibers of its Néron model over $\mathbf{Z}$ are connected. If we identify $J_1(11)/\mathbf{Q}$ and $X_1(11)/\mathbf{Q}$ by the choice of a rational cusp, then $E(1,1)/\mathbf{Z}$ is the minimal regular model of $X_1(11)/\mathbf{Q}$. Note that this discussion provides us with an explicit example of something Brian warned us about in his notes: the morphism $X_1(11)/\mathbf{Q}_{11} \to X_0(11)/\mathbf{Q}_{11}$ does not extend to a morphism of minimal regular models over $\mathbf{Z}_{11}$. (Of course the corresponding morphism of Néron models of $J_1(11)/\mathbf{Q}_{11}$ and $J_0(11)/\mathbf{Q}_{11}$ does extend, but it is not surjective on component groups of the special fibers.)

8.2. **Rational points.** Recall that Bryden undertook some tricky computations in his talk to show that the only rational points on $X_1(11)/\mathbf{Q}$ are the cusps. The information gleaned above about $J_1(11)$ and its reductions is quite enough to perform a simple 5-descent, using flat cohomology to understand the bad places, in the style of [MT74] (cf. [Maz72] for a thorough discussion of the method). From the 5-descent, one deduces that the rank of $J_1(11)(\mathbf{Q})$ (and of $J_0(11)(\mathbf{Q})$) is zero, and even that the Tate-Shafarevich group has no five torsion. More generally, Mazur proves in [Maz72] that any elliptic curve $E/\mathbf{Q}$ with prime conductor p (i.e. good reduction outside of p and stable reduction at p) and non-trivial l-torsion in $E(\mathbf{Q})$ has rank zero.

Granting that the ranks of $J_1(11)(\mathbf{Q})$ and $J_0(11)(\mathbf{Q})$ are zero, let us see that each has exactly five rational points. Reducing modulo 2 and using the Weil bound, one sees that the prime-to-2 part of each group has order ≤ 5. Similarly, reducing modulo 3 shows that the prime-to-3 part has order ≤ 8. The combination of these two bounds and the existence of a point of order 5 in both cases shows that the group of rational points has order exactly 5. In particular, identifying $X_1(11)$ with $J_1(11)$ by the choice of a rational cusp, one sees that the only rational points on $X_1(11)$ are the cusps, i.e. that there are no elliptic curves over $\mathbf{Q}$ with rational points of exact order 11.

For contrast, let us give a proof of this fact (still using rank= 0) based on Mazur's arguments in [Maz78]. This technique works whenever $X_0(p)$ has genus ≥ 1, where such games with Weil bounds are generally not sufficient.

Lemma 8.3. *Let $E/\mathbf{Q}$ be an elliptic curve and $P \in E(\mathbf{Q})$ be a point of exact order* 11*. Then (E,P) has good reduction outside of $p = 2, 11$.*

Proof. Let $p \neq 2, 11$ be a prime. The pair (E,P) determines $y \in Y_0(11)(\mathbf{Q}) \subset X_0(11)(\mathbf{Q}_p) = X_0(11)(\mathbf{Z}_p)$. To begin we want to see $y \in Y_0(11)(\mathbf{Z}_p)$, i.e. that the reduction of y modulo p is not a cuspidal point in $X_0(11)(\mathbf{F}_p)$. Suppose on the contrary that y reduces to a cusp. By applying the Atkin-Lehner involution, we may assume y reduces to the cusp ∞.

Now consider the identification of $X_0(11)/\mathbf{Q}$ with $J_0(11)/\mathbf{Q}$ taking ∞ to the identity for the group law. This identification extends to an isomorphism of $X_0(11)/\mathbf{Z}[1/11]$ and the Néron model of $J_0(11)/\mathbf{Z}[1/11]$ that takes the section ∞ to the identity. As stated above—and this is the crucial point—the rank of $J_0(11)/\mathbf{Q}$ is zero, and so $[\infty] - [y] \in J_0(11)(\mathbf{Q})$ is a non-zero torsion point. (Note, incidentally, that this hypothetical torsion point may have order divisible by p as far as we know.) Since $p \neq 2$, its reduction in $J_0(11)(\mathbf{F}_p)$ is not the identity, by the specialization principle (cf. [Sil86] Chapter VII, Theorem 3.4). Making the identification with $X_0(11)$, this contradicts our assumption that y reduces to ∞.

Consider the point $x \in Y_1(11)(\mathbf{Q}_p)$ determined by (E, P). By the above discussion, it maps to a point in $Y_0(11)(\mathbf{Z}_p) \subset Y_0(11)(\mathbf{Q}_p)$ under the projection $\pi : Y_1(11) \to Y_0(11)$. Since this projection is a finite (and hence proper) map, the valuative criterion tells us that $x \in Y_1(11)(\mathbf{Z}_p)$. Consequently, (E, P) extends to an elliptic curve with section of exact order 11 over $\mathbf{Z}_p$, which is what was to be proved. □

Let $x \in X_1(11)(\mathbf{Q})$ and suppose x is not a cusp. Then x corresponds to a pair (E, P) consisting of an elliptic curve over $\mathbf{Q}$ and a point of exact order 11, and by the lemma, (E, P) has good reduction at all $p \neq 2, 11$. In particular, we can reduce modulo 3 to find an elliptic curve $E/\mathbf{F}_3$ with a point of exact order 11; consequently, $\#E(\mathbf{F}_3) \geq 11$, but the Weil bound assures $\#E(\mathbf{F}_3) \leq 3 + 1 + 2\sqrt{3} < 8$, and so no such x can exist.

Finally, using the isogeny $\phi^\vee : J_0(11) \to J_1(11)$, one can find all the rational points of $J_0(11)$ and hence of $X_0(11)$. Any rational point must map to one of the five points in $J_1(11)(\mathbf{Q})$. The fibers are torsors under $\ker(\phi^\vee) = \mu_5$, the Shimura subgroup. Each fiber contains a rational point, an element of the cuspidal subgroup, and so the fibers (as Galois sets) are all μ_5 and thus contain exactly one rational point. In conclusion, $J_0(11)(\mathbf{Q}) =$ the cuspidal subgroup.

8.3. **Summary.** Let us summarize the properties of $J = J_0(11)/\mathbf{Q}$ that we have found:

1. J has good reduction outside of 11
2. J has multiplicative reduction at 11. The modulo-11 fiber of the Néron model has five components.
3. The point $[0] - [\infty] \in J(\mathbf{Q})$ generates a subgroup of order 5, the cuspidal subgroup. The reduction of the cuspidal subgroup modulo 11 generates the component group of the modulo-11 fiber of the Néron model.
4. The kernel of the isogeny $\phi^\vee : J_0(11) \to J_1(11)$ is isomorphic to μ_5 and is called the Shimura subgroup.
5. The torsion subgroup of $J(\mathbf{Q})$ is the cuspidal subgroup.
6. The rank of $J(\mathbf{Q})$ is zero.

In [Maz77], Mazur proves generalizations of all of these statements for $J_0(N)$ with N a prime, whenever this abelian variety has positive dimension. Evidently, N replaces 11 in the above list. The number 5 must be replaced by the numerator n of $(N-1)/12$. In (4.), one considers the maximal étale extension $X_2(N)/X_0(N)$ contained in $X_1(N)/X_0(N)$; the cover $X_2(N) \to X_0(N)$ is cyclic Galois of degree n, as can be checked by computing the ramification of $X_1(N)/X_0(N)$. The corresponding kernel of $J_0(N) \to J_2(N)$ is called the Shimura subgroup of $J_0(N)$; it is again isomorphic to μ_n. Finally, in (5.), it is rarely true that $J_0(N)(\mathbf{Q})$ has rank zero, but Mazur produces a quotient abelian variety, the Eisenstein quotient, which does have rank 0. The proof that the rank is 0 is a collection of infinite l-descents, where l runs over the prime divisors of n. (For l odd, one can make a simple descent generalizing the simple 5-descent that can be used for $J_0(11)$ and $J_1(11)$.) The L-function of the Eisenstein quotient does not vanish at 1, and so Mazur's descent can be considered a verification of a case of the rank part of the Birch-Swinnerton-Dyer conjecture. This much of Mazur's paper has been superseded by more recent results using Euler systems, another descent technique.

There are a couple of loose ends to tie up:

1. There is one more elliptic curve of conductor 11 that comes out of the above discussion, namely the quotient J' of $J_0(11)$ by its cuspidal subgroup. The image of the Shimura subgroup provides a copy of $\boldsymbol{\mu_5}$ in J', and the only rational point on J' is the identity. One immediately obtains the μ_5 version of Proposition 8.1: the only elliptic curves over $\mathbf{Q}$ with good reduction outside of a single prime p that contain a copy of μ_5 are $J_0(11)$ and J'.
2. As proved above, the curve $X_0(11)$ has five rational points. Two are the cusps 0 and ∞. The remaining three points can be identified: the abelian variety $J_0(121)$ decomposes (up to isogeny) as $J_0(11)^2$, the "old part," and a 4-dimensional "new part." The new part is isogenous to a product of four elliptic curves. One is the (isogeny class of the) (-11)-twist of $J_0(11)$. The other three factors admit rational 11-isogenies. One is an elliptic curve E with potential complex multiplication by $\mathbf{Z}[(1 + \sqrt{-11})/2]$; it is 11-isogenous to its (-11)-twist. The other two factors are (the isogeny class of) an elliptic curve E' and (the isogeny class of) its (-11)-twist. The three anomalous rational points of $X_0(11)$ correspond to E, E', and the quotient of E' by its rational cyclic subgroup of order 11. (Twisting a pair (E, C) does not change the associated point

on $X_0(11)$.) I checked the non-evident claims above using the Eichler-Shimura construction and the online tables of William Stein. Perhaps one ought to be able to verify such things without tables.

9. Appendix: some representability results

Before proving the main representability results, let us recall a few basic facts.

9.1. **Weierstrass equations.** Let E/S be an elliptic curve (i.e. an abelian scheme of relative dimension 1). The sheaf $f_*\Omega^1_{E/S}$ of global invariant differentials on E/S is locally free. If ω is a generating section of this sheaf (which, of course, need not exist globally on S) and S is affine, one can associate (by the usual procedure) a Weierstrass equation for E/S, well-defined up to an (r,s,t) transformation, where $r,s,t,\in\Gamma(S,\mathcal{O}_S)$. If one allows a change $\omega = u\omega'$ for $u\in\Gamma(S,\mathcal{O}_S)^\times$, then the Weierstrass equation is well-defined up to a (u,r,s,t) transformation. Conversely, if E/S is defined by a Weierstrass equation (with $a_1,\dots,a_6\in\Gamma(S,\mathcal{O}_S)$, then

$$\omega = \frac{dx}{2y+a_1x+a_3}$$

is a generator of $f_*\Omega^1_{E/S}$. Consequently, the existence of a Weierstrass equation (over affine S) is equivalent to the existence of a generating section of $f_*\Omega^1_{E/S}$.

9.2. **Sheaves on** (Schemes)**.** The various functors F : (Schemes) → (Sets) that we want to represent have an additional useful property that can be established *a priori.* Let F be any such functor. We say that F is a *Zariski sheaf of sets* on (Schemes), if for each scheme S, the restriction of F to the (Zariski) open sets of S is a sheaf. The simplest example of a Zariski sheaf of sets is a representable functor $F(S) = \mathrm{Hom}(S,Y)$; the sheaf property encodes the standard facts about gluing morphisms of schemes.

This property is easy to check in our situation: the master functor is defined by

$$F(S) = \{(E,P) : E/S \text{ is an elliptic curve}, P\in E(S) \text{ not of order } 1,2, \text{ or } 3 \text{ in any geometric fiber}\}/\approx .$$

Any such pair (E,P) has no automorphisms—in other words, if (E,P) and (E',P') are isomorphic, there is a unique isomorphism between them: the structure of the automorphisms of E/S is known (cf. [Del75]), and one sees that the only cases in which $\sigma P = P$ for an automorphism σ occur when P has order 1, 2, or 3.

Now consider an open cover $\{U_i\}$ of S. If $x,x'\in F(S)$ corresponding to (E,P) and (E',P') restrict to the same elements of $F(U_i)$ for each i, then the isomorphisms of $(E,P)|U_i$ and $(E',P')|U_i$ glue together to give a global isomorphism since over each U_i there is a unique choice of isomorphism. Similarly, if one has elements $x_i\in F(U_i)$ with agreement for each pair (i,j) of the restrictions in $F(U_i\cap U_j)$, then any corresponding local structures (E_i,P_i) on U_i glue to give a global (E,P) on S by the uniqueness of isomorphisms.

9.3. **Representability.** Let F : (Schemes) → (Sets) be the functor defined in the previous paragraph. Here is the master result:

Theorem 9.1. *The functor F is represented by the scheme $Y = \mathrm{Spec}(\mathbf{Z}[B,C,\Delta(B,C)^{-1}]$ with universal pair $(E(B,C),(0,0))$.*

Proof. As in the general discussion of representable functors, the pair $(E(B,C),(0,0))$ over Y defines a natural transformation $Y\Rightarrow F$. We want to see that this natural transformation is in fact a natural isomorphism.

First let us check that for each scheme S, the map $Y(S)\to F(S)$ is injective. Let us unwind what this injectivity means: a morphism $S\to Y$ is defined by giving $b,c\in\Gamma(S,\mathcal{O}_S)$ such that $\Delta(b,c)\in\Gamma(S,\mathcal{O}_S)^\times$. To say that two elements of $Y(S)$ corresponding to (b,c) and (b',c') determine the same element of $F(S)$ is to say that $(E(b,c),(0,0))$ and $(E(b',c'),(0,0))$ are isomorphic over S. Any such isomorphism must come from a (u,r,s,t)-type transformation of the Weierstrass equations, but, as in §1, there are no such transformations unless $b=b'$ and $c=c'$.

Since Y and F are known to be a Zariski sheaves of sets, to finish the proof that each map $Y(S)\to F(S)$ is an isomorphism, it suffices to see that for each scheme S, the map $Y|S\to F|S$ of the restrictions of Y and F to open sets in S is a surjective map of sheaves. In other words, we must see that for any $x\in F(S)$, there is a Zariski open cover $\{U_i\}$ of S such that for each i, the element $x|U_i \in F(U_i)$ is the image of something in $Y(U_i)$. It suffices, therefore, to prove that any $(E,P)/S$ that has a Weierstrass equation (which can be arranged Zariski-locally) is isomorphic to some $(E(b,c),(0,0))$.

For an (E,P) with a Weierstrass equation, one can choose a (u,r,s,t) transformation to put (E,P) in the form $(E(b,c),(0,0))$ exactly as in Bryden's talk. In brief, one translates P to $(0,0)$ (using r and t), makes $y=0$ the tangent line at P (using s), and makes a u-transformation to arrange $a_2 = a_3$. To perform these three steps one must know (in order) that P does not have order 1, 2, or 3. □

Using the universal pair $(E(B,C),(0,0))$ above, one can prove other representability results. For instance, for an integer $N \geq 4$, let $Y_N \to Y$ be the pullback of the diagonal of $E(B,C) \times_Y E(B,C)$ under the map $O \times [N](0,0)$ (where O is the identity section of $E(B,C)$). Then Y_N with the restriction of $(E(B,C),(0,0))$ evidently classifies pairs (E,P), where E/S is an elliptic curve and $P \in E(S)$ is not of order $1,2$, or 3 in any geometric fiber and satisfies $[N]P = O$. (To be precise, the natural transformation $Y \Rightarrow F$ maps $Y_N(S)$ to the subset of classes of (E,P) in $F(S)$ satisfying $[N]P = O$.) Taking the complement of Y_d in Y_N, where d runs over proper divisors of N (with the pullback of $(E(B,C),(0,0))$) then gives an object representing the functor F_N defined in §3 (with the domain extended to all schemes, in fact), proving Proposition 3.1.

Concretely, this proof of representability gives the following recipe for constructing $Y_1(N)$: write down the Tate-normal-form curve and compute $[d](0,0)$ for all divisors d of N. Each condition $[d](0,0) = O$ provides an algebraic relation between B and C. The curve $Y_1(N)$ is obtained by imposing the condition $[N](0,0) = O$ and excluding the conditions $[d](0,0) = O$ for all proper divisors d of N. (Recall that $[1](0,0) = O$, $[2](0,0) = O$, and $[3](0,0) = O$ are excluded by construction.) If N is prime, for instance, there are no conditions to exclude.

10. Exercises

10.1. **An alternative construction of $X_1(N)$.** Work out the following alternative compactification of $Y_1(N)/\mathbf{Z}[1/N]$ for $N \geq 5$ prime. The motivation is the observation that for N prime, the two packets of cusps, 1-gons and N-gons, are switched by Atkin-Lehner involutions.

1. Using Weierstrass equations as in the previous section, construct a scheme Y^* representing the functor on $\mathbf{Z}[1/N]$-schemes S whose S-points are the isomorphism classes of triples $(E/S,O,P)$ where E/S is proper, finitely presented, and flat with each geometric fiber either an elliptic curve or a nodal cubic; O and P are sections of E^{sm}/S, the smooth locus; and P has exact order N in E^{sm}/S, where E^{sm} is given the structure of a group scheme with identity section O in the usual way. Note that the usual definition of diamond operators $\langle a \rangle$ applies to give an action of $(\mathbf{Z}/N\mathbf{Z})^\times$ as automorphisms of Y^*.
2. Working over $\mathbf{Z}[1/N,\zeta_N]$, define a scheme X_a for each $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ by gluing two copies of Y^* along $Y_1(N) \subset Y^*$ using the Atkin-Lehner involution $w_{\zeta_N^a}$.
3. Verify that $X_a/\mathbf{Z}[1/N,\zeta_N]$ is proper by using the valuative criterion.
4. Using the diamond operators, construct a coherent system of isomorphisms among the $X_a/\mathbf{Z}[1/N,\zeta_N]$. These isomorphisms provide (effective) descent data on the X_a from $\mathbf{Z}[1/N,\zeta_N]$ to $\mathbf{Z}[1/N]$ and hence a compactification $X_1(N)/\mathbf{Z}[1/N]$ of $Y_1(N)/\mathbf{Z}[1/N]$.
5. Check any basic property of $X_1(N)/\mathbf{Z}[1/N]$ (e.g. smoothness) that occurs to you.

10.2. **Miscellaneous.** Here are a few more exercises culled from the above exposition.

1. Compute the minimal Weierstrass model of $E(T,0)$ over $\mathbf{Q}[T,1/\Delta(T,0)]$ at $T=0$, $T=-1/16$, and $1/T=0$. Note that there is additive reduction at one of these places, in contrast with the degeneration of the universal curve over $Y_1(5)$ (and, for that matter, $Y_1(N)$ for $N>5$) worked out in §4.
2. Look up the functorial criterion for smoothness and use it to verify that $Y_1(N)/\mathbf{Z}[1/N]$ is smooth.
3. Using the theory of Weierstrass equations for relative elliptic curves outlined above, construct a relative j-invariant: for each E/S an elliptic curve, produce $j(E/S) \in \Gamma(S,\mathcal{O}_S)$ functorial in E/S such that if $S = \mathrm{Spec}(\mathbf{C})$, then $j(E/S)$ is the classical j-invariant. (You must unwind how the usual $j \in \mathbf{Z}[a_1,a_2,a_3,a_4,a_6,\Delta^{-1}]$, which is an invariant for the action of the algebraic group of (u,r,s,t)-transformations, provides a solution—the unique solution— to the problem.)

4. The previous exercise defines a natural transformation from the functor whose S-points are isomorphism classes of elliptic curves over S to the functor of S-points of $\mathbf{A}^1$. Prove that $\mathbf{A}^1/\mathbf{Z}$ is the coarse moduli scheme for this moduli functor. Prove the same fact about $\mathbf{A}^1/T$ and the moduli of elliptic curves over T-schemes S, where T is any base scheme. The concrete version of the problem is to show that the ring of invariants of $R[a_1, a_2, a_3, a_4, a_6, \Delta^{-1}]$ under the algebraic group of (u, r, s, t) transformations is $R[j]$, where R is any commutative ring. You should be able to do this for $R = \mathbf{Z}$ (or, just as well, for $R = \mathbf{C}$) at least.
5. For N prime, check the description of $\mathrm{Cusps}_1(N)/\mathbf{Z}[1/N]$ given in §5 by using the modular description.
6. Prove that $[n] : E \to E$ is an isogeny for E/S an elliptic curve and $n \neq 0$ an integer.
7. Prove the existence of the schemes Isog_n discussed in §6. It may help to consider the refined problem of constructing a scheme over $\mathbf{Z}[1/N]$ parameterizing isogenies $\phi : (E, P) \to (E', P')$ such that $\ker(\phi)$ is locally isomorphic to a product of cyclic groups of order $n_1, \dots, n_r$ with $n_1 \times \ldots \times n_r = n$.
8. (a) Let E be an elliptic curve over a field K (possibly of non-zero characteristic). Prove that there are finitely many N-isogenies with source E for any positive integer N.
(b) On the other hand, let E be a supersingular elliptic curve over $\overline{\mathbf{F}}_p$. Show that there are infinitely many p-isogenies with source $E \times E$.
(c) Prove that $\mathrm{Isog}_p^0/\mathbf{F}_p$ is dense in $\mathrm{Isog}_p/\mathbf{F}_p$. It would suffice to show that any p-isogeny can be deformed to an ordinary p-isogeny. (You may find this a bit tricky.)
9. Prove the relation $(T_p)_* = F + F^\vee$ in $\mathrm{End}(J_0(N)/\mathbf{F}_p)$ using a suitable version of the Kronecker(-Eichler-Shimura) congruence relation. Here $N \geq 5$ is an integer, and p is a prime that does not divide N. The endomorphism F is Frobenius, and $F^\vee$ is the dual of Frobenius with respect to the canonical principal polarization. It may be helpful to look at a discussion a correspondences on curves and Jacobians (cf. [Shi94] or [Mil86]).
9. Explain how to construct a rational point on $X_0(11)$ using the elliptic curve $E/\mathbf{C}$ with complex multiplication by $\mathbf{Z}[(1+\sqrt{-11})/2]$. (Note that there is only one such curve up to isomorphism since the class number of $\mathbf{Q}(\sqrt{-11})$ is 1.) More generally, explain how to construct a rational point on $X_0(N)$, if $N \equiv 3 \pmod 4$ is prime and the class number of $\mathbf{Q}(\sqrt{-N})$ is 1. Consequently, the class-number-1 problem is contained in the problem of determining the rational points on the curves $X_0(N)$.
10. Use the methods of [MT74] to perform simple 5-descents on $E(1,1)$ and $E(11,11)$ and simple 4- or 2-descents (your choice) on $E(1,0)$ and $E(-1,0)$ (all of this over $\mathbf{Q}$). What are the ranks of these elliptic curves? It may be helpful to use the structure of the bad reduction in each case. If you can not figure this out, take a look at [Maz72].
11. By any means you can (using tables, for example), verify the claims about $X_0(11)(\mathbf{Q})$ and $J_0(121)$ made at the end of §8.

References

[Con95] Ian Connell, *Points of order 11 on elliptic curves*, Nieuw Arch. Wisk. (4) **13** (1995), no. 3, 257–288.

[Del75] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 53–73. Lecture Notes in Math., Vol. 476.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Igu59] Jun-ichi Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561–577.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[MT74] B. Mazur and J. Tate, *Points of order 13 on elliptic curves*, Invent. Math. **22** (1973/74), 41–49.

[Ray67] M. Raynaud, *Passage au quotient par une relation d'équivalence plate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 78–85.

[Ray74] Michel Raynaud, *Schémas en groupes de type $(p,\dots,p)$*, Bull. Soc. Math. France **102** (1974), 241–280.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.