Towards Defining a Stack of Elliptic Curves

Yannick Van Huele

11 December 2011

1 Introduction

The goal of this project was to read Dan Edidin's article *What is a Stack?* [8] and then fill in enough details to make the article accessible to anyone taking Math 581g. This goal depended on my ability to fill in enough details so that the article became accessible to me, something I ultimately failed to achieve. However, I have tried to fill in what gaps I could, in the hopes that someone with the same goal could use this paper as a stepping stone.

As the goal of this paper is understanding Edidin's article, it makes sense to state the motivation behind Edidin's article. Edidin begins:

> A Riemann surface of genus 1 is homeomorphic to the torus $T = S^1 \times S^1$. Therefore, a choice of a point to be the origin determines a group structure on the Riemann surface. An *elliptic curve* is a Riemann surface of genus 1 together with a choic of origin for the group structure. Although all elliptic curves are homeomorphic to the topological group $S^1 \times S^1$, they may have nonisomorphic complex structures. A natural question, called the problem of moduli, is to describe the space of all possible isomorphism classes of objects of a certain type. In this article we discuss this question for elliptic curves and explain how we are led to consider the notion of *stacks*.
>
> We wish to construct a *moduli space* for elliptic curves. Points of the moduli space should correspond to isomorphism classes of elliptic curves.

Thus, this paper will also aim at constructing a moduli space for elliptic curves. I begin with a discussion of the j-invariant of an elliptic curve. Two elliptic curves are isomorphic over $\mathbb{C}$ if and only if they have the same j-invariant. This makes $\mathbb{C}$ seem a natural choice for the moduli space of elliptic curves and so I felt some discussion of the j-invariant would be useful. In class we gave one definition of the j-invariant. Edidin provides a different definition, which I had not previously seen. Referring to Silverman's book [10], I argue that the definitions are equivalent and state some useful results about the j-invariant. In the second section, I introduce families of elliptic curves and the notion of a universal family. Then, following a post on mathoverflow.net [6], I construct an isotrivial family of elliptic curves and argue that $\mathbb{C}$ cannot be the moduli space of elliptic curves. Finally, I give Edidin's construction of the stack of elliptic curves, but do not prove that it is in fact the moduli space of elliptic curves.

When looking up material to try and understand the article, I frequently ran into mathematical objects I had little or no familiarity with and was not able to gain the familiarity which would allow me to use them confidently. Thus, I have tried to indicate places where my arguments lack rigor. Given that I was not able to flesh out Edidin's article to my own satisfaction, I have also tried to

indicate what further clarifications would be helpful for me, as a student in Math 581g, in better understanding the article.

2 The j-invariant

Definition 2.1. *Given an elliptic curve E with Weierstrass equation*

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

let b_2, b_4, b_6, b_8, c_4, and Δ be the quantities

$$\begin{array}{lcllcl} b_2 &=& a_1^2 + 4a_2 & b_8 &=& a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ b_4 &=& 2a_4 + a_1a_3 & c_4 &=& b_2^2 - 24b_4 \\ b_6 &=& a_3^2 + 4a_6 & \Delta &=& -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{array}$$

We define the j-invariant $j(E)$ of E to be the quantity

$$j = \frac{c_4^3}{\Delta}$$

The usefulness of the j-invariant in classifying elliptic curves comes from the following result:

Proposition 2.2. *Let K be a field. Then two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant. Furthermore, for each $j_0 \in \bar{K}$, there exists an elliptic curve E defined over K such that $j(E) = j_0$.*

Proof: See Chapter 3 of [10]

In class we defined the j-invariant for an elliptic curve E (over $\mathbb{C}$) with equation $E : y^2 = 4x^3 - g_2x - g_3$ to be given by

$$\frac{1728g_2^3}{g_2^3 - 27g_3^2}$$

(See Chapter 11 of [9].) Substituting $y \mapsto 2y$ into the equation for E, we obtain

$$E' : y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$$

This is a Weierstrass equation of the form used in definition 2.1 and so we may compute its j-invariant. We have

$$a_1 = a_3 = a_2 = 0, \quad a_4 = -\frac{g_2}{4}, \quad \text{and} \quad a_6 = -\frac{g_3}{4}$$

Thus

$$\begin{array}{lcllcl} b_2 &=& 0 & b_8 &=& -\dfrac{g_2^2}{16} \\ b_4 &=& -\dfrac{g_2}{2} & c_4 &=& 12g_2 \\ b_6 &=& -g_3 & \Delta &=& g_2^3 - 27g_3^2 \end{array}$$

and we see that

$$j(E') = \frac{c_4^3}{\Delta} = \frac{(12g_2^2)^2}{g_2^3 - 27g_3^2} = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$$

The map $(x, y) \mapsto (x, 2y)$ defines an isomorphism of elliptic curves, so by Proposition 2.2, $j(E) = j(E')$. Thus, we see that the two definitions of the j-invariant agree (when both make sense). It will be useful later to have the following result. Let K be a field and let E be an elliptic curve defined over K with equation $E : y^2 = x^3 + ax + b$. Let $d \in K^\times$ and let E' be the elliptic curve defined over K with equation $E' : dy^2 = x^3 + ax + b$ (E' is a quadratic twist of E).

Fact 2.3. *E and E' are isomorphic over $K(\sqrt{d})$, but not over K if $K \neq K(\sqrt{d})$.*

The j-invariant presented in Edidin's paper is defined differently from those above. However, his definition agrees with the other two:

Proposition 2.4. *Let E be an elliptic curve over a field K with $\mathrm{char}(K) \neq 2$. Then there exists $\lambda \in \bar{K} \backslash \{0, 1\}$ such that E is isomorphic over $\bar{K}$ to the curve E_λ given by*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

This curve E_λ is said to be in Legendre form. Furthermore, the j-invariant of E_λ is given by

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

and the association

$$\begin{array}{rcl} \bar{K} \backslash \{0, 1\} & \to & \bar{K} \\ \lambda & \mapsto & j(\lambda) \end{array}$$

is surjective and is exactly six-to-one except above $j = 0$ and $j = 1728$.

Proof: See Chapter 3 of [10]

3 Coarse Moduli Space

Proposition 2.2 tells us that two elliptic curves are isomorphic over $\mathbb{C}$ if and only they have the same j-invariant and that every $z \in \mathbb{C}$ is the j-invariant of some curve. In this sense, $\mathbb{C}$ seems like a good candidate to be the moduli space of elliptic curves over $\mathbb{C}$. However, we would like our moduli space to have an additional property which $\mathbb{C}$ lacks. To describe this property, we need to first introduce some more definitions. Following Edidin, let us define families of elliptic curves:

Definition 3.1. *A family of elliptic curves over a base space B is a fibration $\pi : X \to B$ with a section $O : B \to X$ (i.e., a right inverse $\pi \circ O = \mathrm{id}_B$) such that for every $b \in B$ the fiber $\pi^{-1}(b)$ is an elliptic curve with origin $O(b)$.*

I struggled for a while with this definition and am not yet completely comfortable with it, so let me unwind (hopefully without completely misinterpreting) what this means. First, note that elements

of X are not elliptic curves, but instead points on an elliptic curve. The elliptic curves correspond to the fibers of π:

$$\pi^{-1}(b) = \{x \in X : \pi(x) = b\} \ni O(b)$$

Next, I'll admit that I do not know what is meant by a fibration. Later in the article, Edidin makes it clear that $\pi : X \to B$ is a map of varieties. There is a Wikipedia article on fibrations [1]. However, it was pointed out to me that the definition presented there involves a map in the category of topological spaces rather than the category of algebraic varieties. I will present this definition and leave it to a more ingenious reader to determine the appropriate analogue in the category of algebraic varieties, if such an analogue exists. (Here it may be worthwile to note that there also exist fibred categories [2], and that the term fibration may stem from there instead.) According to Wikipedia, a fibration is a continuous map $\pi : X \to B$ satisfying the homotopy lifting property with respect to every space Y. That is, given a homotopy $H : Y \times [0,1] \to B$ and a lift $\tilde{H}_0 : Y \to X$ of $H_0(y) = H(y,0)$ making the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\tilde{H}_0} & X \\ {\scriptstyle \mathrm{id}_Y \times \{0\}}\downarrow & & \downarrow{\scriptstyle \pi} \\ Y \times [0,1] & \xrightarrow{H} & B \end{array}$$

commute, there exists a lift $\tilde{H} : Y \times [0,1] \to X$ such that $\pi \circ \tilde{H} = H$ and $\tilde{H}_0(y) = \tilde{H}(y,0)$.

Given an family of elliptic curves $\pi : X \to B$, let us define a classifying map $j_B : B \to \mathbb{C}$ by

$$j_B(b) = j(\pi^{-1}(b))$$

Now, let us give one more definition:

Definition 3.2. *Let $\mathcal{C}$ be a category, let X, Y, and Z be objects of C such that there exist morphisms $f : X \to Z$ and $g : Y \to Z$. The pullback of $f : X \to Z$ and $g : Y \to Z$ is an object P along with two morphisms $p_1 : P \to X$ and $p_2 : P \to Y$ such that the diagram*

$$\begin{array}{ccc} P & \xrightarrow{p_2} & Y \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & Z \end{array}$$

commutes and such that, given any object $Q \in \mathcal{C}$ and pair of morphisms $q_1 : Q \to X$ and $q_2 : Q \to Y$ such that the diagram

$$\begin{array}{ccc} Q & \xrightarrow{q_2} & Y \\ {\scriptstyle q_1}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & Z \end{array}$$

commutes, there exists a unique morphism $r : Q \to P$ such that $q_1 = r \circ p_1$ and $q_2 = r \circ p_2$. If the pullback exists, it is unique up to isomorphism.

The additional condition we wish a moduli space to satisfy is that there should exist a universal family $\pi_{\mathcal{E}} : \mathcal{E} \to \mathbb{C}$ such that every family of elliptic curves $\pi : X \to B$ is obtained by pulling back $j_B : B \to \mathbb{C}$ and $\pi_{\mathcal{E}} : \mathcal{E} \to \mathbb{C}$:

$$\begin{array}{ccc} X & \longrightarrow & \mathcal{E} \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi_{\mathcal{E}}} \\ B & \xrightarrow{j_B} & \mathbb{C} \end{array}$$

However, no such universal family exists. To see why, consider the following example given as an answer to a question on mathoverflow.net [6]. (The original example was described in terms of schemes and I have tried to reinterpret it in a way that makes sense to me so I will give my standard warning about the potential for mistakes in what follows.) Let E_0 be an elliptic curve over $\mathbb{Q}$ with equation $E_0 : y^2 = x^3 + ax + b$. For each $d \in \mathbb{Q}^\times$, let E_d denote the elliptic curve over $\mathbb{Q}$ given by $E_d : dy^2 = x^3 + ax + b$ (so $E_1 = E_0$). Now, let X, X_0 be the spaces

$$X = \bigsqcup_{d \in \mathbb{Q}^\times} E_d \qquad \text{and} \qquad X_0 = \bigsqcup_{d \in \mathbb{Q}^\times} E_0 = E_0 \times \mathbb{Q}^\times$$

(here $\sqcup$ denotes the disjoint union) and let $\pi : X \to \mathbb{Q}^\times, \pi_0 : X_0 \to \mathbb{Q}^\times$ be the projections onto $\mathbb{Q}^\times$: for each $p \in E_d$, $p_0 \in E_0$

$$\pi(p, d) = d \qquad \text{and} \qquad \pi_0(p_0, d) = d$$

Then, for each $d \in \mathbb{Q}^\times$

$$\pi^{-1}(d) = E_d \times \{d\} \cong E_d \qquad \text{and} \qquad \pi_0^{-1}(d) = E_0 \times \{d\} \cong E_0$$

Finally, letting $O : \mathbb{Q}^\times \to X$ and $O_0 : \mathbb{Q}^\times \to X_0$ denote the sections mapping $d \in \mathbb{Q}^\times$ to the origin of E_d and E_0, respectively, we see that $\pi : X \to \mathbb{Q}^\times$ and $\pi_0 : X_0 \to \mathbb{Q}^\times$ are two families of elliptic curves. Note that, by Fact 2.3 and Proposition 2.2, both families induce the same classifying map, namely the constant map $j_{\mathbb{Q}^\times} : \mathbb{Q}^\times \to \mathbb{C}$, $d \mapsto j(E_0)$:

$$d \mapsto j(\pi^{-1}(d)) = j(E_d) = j(E_0) = j(\pi_0^{-1}(d)) \hookleftarrow d$$

However, the two families are not equivalent. The family $\pi_0 : X_0 \to \mathbb{Q}^\times$ is trivial: for all $d_1, d_2 \in \mathbb{Q}^\times$, the elliptic curves $\pi_0^{-1}(d_1)$ and $\pi_0^{-1}(d_2)$ are isomorphic over $\mathbb{Q}$. However, the family $\pi : X \to \mathbb{Q}^\times$ is isotrivial: the j-invariant of each elliptic curve $\pi^{-1}(d)$ is the same, but by Fact 2.3, we see that there exist $d_1, d_2 \in \mathbb{Q}^\times$ such that the curves $\pi^{-1}(d_1)$ and $\pi^{-1}(d_2)$ are not isomorphic over $\mathbb{Q}$. In particular, we see that the isomorphism classes of the fibers $\pi^{-1}(d)$ over $\mathbb{Q}$ are in bijection with $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Thus, there cannot exist a universal family $\pi_{\mathcal{E}} : \mathcal{E} \to \mathbb{C}$. For otherwise, both X and X_0 would be obtained by pulling back $\pi_{\mathcal{E}} : \mathcal{E} \to \mathbb{C}$ and $j_{\mathbb{Q}^\times} \to \mathbb{C}$, but we have seen that these families are not isomorphic. Hence, $\mathbb{C}$ is not the moduli space of elliptic curves. However, insofar as points in $\mathbb{C}$ correspond to isomorphism classes of elliptic curves via the j-invariant, we call $\mathbb{C}$ the *coarse moduli space* of elliptic curves.

4 Stacks

As $\mathbb{C}$ does not quite work, we need to turn elsewhere in our search for the moduli space of elliptic curves. For the answer, we turn to stacks.

Let $\mathcal{M}$ denote the category with the following objects and morphisms: an object of $\mathcal{M}$ is a family of elliptic curves $\pi : X \to B$ and a morphism of $\mathcal{M}$, $(\pi' : X' \to B') \to (\pi : X \to B)$, is a pair of maps, $e : X' \to X$ and $\beta : B' \to B$, such that the diagram

$$\begin{array}{ccc} X' & \xrightarrow{e} & X \\ {\scriptstyle \pi'}\downarrow & & \downarrow{\scriptstyle \pi} \\ B' & \xrightarrow{\beta} & B \end{array}$$

commutes and X' is isomorphic to the pullback of X via the map $\beta : B' \to B$. We call $\mathcal{M}$ the stack of elliptic curves. The subcategory of $\mathcal{M}$ corresponding to families over a fixed base B is called the fiber over B.

$\mathcal{M}$ is an example of an algebraic stack, which Edidin defines as follows:

Definition 4.1. *An algebraic stack is a category fibered in groupoids which has a smooth covering by an affine variety.*

$\mathcal{M}$ also turns out to be the moduli space of elliptic curves and Edidin constructs the universal family $\mathcal{C} \to \mathcal{M}$ where $\mathcal{C}$ is a category whose objects are families of elliptic curves with a section and morphisms defined the same way as for $\mathcal{M}$. The map $\mathcal{C} \to \mathcal{M}$ is the forgetful functor, taking a family with a section to the same family without the section. I will not try and recreate this argument as I do not understand it.

5 Final Comments

A useful contribution towards clarifying the rest of Edidin's argument would be an explanation of how the functor $\underline{B} \to \mathcal{M}$ is defined. Given a map of varieties $t : T \to B$, how does one obtain the corresponding family of elliptic curves $\pi : X \to B$?

Finally, for those interested in learning more about stacks, a guide to the literature can be found at the Stacks Project [5]. (Though it should be noted that Edidin's article was the least technical of those I found there.)

References

[1] Wikipedia entry on Fibration. http://en.wikipedia.org/wiki/Fibration.

[2] Wikipedia entry on Fibred category. http://en.wikipedia.org/wiki/Fibred_category.

[3] Wikipedia entry on Moduli space. http://en.wikipedia.org/wiki/Moduli_space.

[4] Wikipedia entry on Pullback (category theory). http://en.wikipedia.org/wiki/Pullback_%28category_theory%29.

[5] The Stacks Project Authors. Stacks project. http://math.columbia.edu/algebraic_geometry/stacks-git.

[6] basic (mathoverflow.net/users/1238). (nontrivial) isotrivial family of elliptic curves. MathOverflow. http://mathoverflow.net/questions/12500 (version: 2010-01-21).

[7] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[8] Dan Edidin. What is a stack? *Notices of the AMS*, 50(4):458–459.

[9] Kenneth A. Ribet and William A. Stein. Lectures on modular forms and Hecke operators. http://wstein.org/edu/2011/581g/ribet-stein/main.pdf, 2011.

[10] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd. edition, 2009.