Families of Elliptic Curves: Non Singular Models

Michael Szydlo

August 15, 2000

Contents

1 Introduction

I present some topics about families of Elliptic curves. This has historically been a fruitful way to understand their arithmetic structure. In particular, I researched methods of constructing non-singular models for families of elliptic curves. This research was fundamental and not aimed at any application. However thinking about elliptic in this way will be useful for practical applicatons as well. I organize the slides as follows:

- Elliptic Curves (My Intro Version)
- Families of Elliptic Curves (Parameter Space)
- Models of Elliptic Curves (Group and fibers)
- Constructing Models (Schemes by others)
- A Theorem (My research)
- $J = 0$ families (Testing ground)
- Some Kodaira Types (Fiber examples: beyond cusp)
- Higher Dimensions (The fiber's meet)
- Limiting Collision Types (Eliminate incompatible ones)
- The Regular model (Summary of Construction)
- Research on Curves (Uses, related research)

2 Elliptic Curves

- Complex Tori, Algebraic Curves.
- Abelian Groups, Weierstrass Equations.
- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- $x, y, a_i \epsilon K$, K any field.
- K finite $\rightarrow$ E is finite group.
- Number Theory - Fermat.
- Physics - Calibi Yau Manifolds (Strings).
- Cryptography: #E has big prime factor.
- Discrete Log is Difficult: $P_1 = nP_2$.
- Examples (CM curves).

$y^2 = x^3 + tx$ over F_p with $p = 1$ (mod 4)

$y^2 = x^3 + t$ over F_p with $p = 1$ (mod 6)

- Those are Families of Elliptic Curves.

3 Families of Elliptic Curves

- Add a parameter t to the a_i.
- Parameterize by an Algebraic Variety.
- $y^2 = x^3 + tx$ for $t \epsilon F_p$, $\quad V = Spec(F_p[t])$.
- Fibers: One curve for each Prime ideal of R.
- Examples of Bases

One dimensional: $C[t], Z, F_p[t]$.

Two dimensional: $C[s,t], Z[t], F_p[s,t]$.

Three dimensional: $C[t_1, t_2, t_3, ...t_n], Z[s,t], Z_p[s,t]$.

Global: Variety or Scheme, Locally given by a Ring.

- Base has dim $=k \rightarrow$ Family has dim $= k+1$.
- Notation: $E \rightarrow B$, $\;$ Fibers : $E_p \;\; p \epsilon B$.
- Generalize Discriminant: (Polynomial in a_i).
- Discriminant defines a Divisor on B.
- $y^2 = x^3 + Ax + B$ has discriminant $16(4A^3 + 27B^2)$.
- Disc($y^2 = x^3 + st$) is defined by $s^2 = 0$ and $t^2 = 0$.
- This Divisor is two double lines intersecting in a point.

4 Models of Elliptic Curves

- Fibers of Family at a point on Discriminant are not Elliptic Curves.
- Interest in comparing fibers of the family (#E, structure).
- Singular fibers may be cusps or nodes.

$$y^2 = x^3$$

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

- Question: Is the family itself smooth?
- Can we give group structure to singular fibers?

  Removing cusp or node from E/K. It is a group.

  Example: $y^2 = x^3 + x^2$ over F_p is cyclic of order p.
- Model of an Elliptic Curve:

An Variety over a base B with generic fiber an Elliptic Curve. It may have properties : flat, regular, minimal, proper.

- The curve $y^2 = x^3+2x^2+6$ over $Spec(Z)$ is a model.
- Over Q, and most primes it is an Elliptic Curve.
- Over 2 it is a cusp, Over 3 it is a node.

5 Constructing Models

- Nice Models: Flat, Regular, Proper, Minimal*.
- The arithmetic of the fibers should be related.
- Defining a Group Scheme (composition and inverse).

$$E \times E \to E$$

$$E \to E$$

These are morphisms of *schemes* over the Base.

- Means: Same equations define group law for all fibers. These morphisms restrict to fibers giving group law.
- Néron model: A Smooth Group Scheme.

  A smooth proper regular minimal model of family E.

  Theorem: They Exist when B is a curve (DVR)

  Comes from Weierstrass Equations

  Has some singular fibers (cusp or node) replaced.
- These Schemes can be constructed Algorithmically.

  Start with a scheme defined by Weierstrass Equations Replace some singular fibers via a *Blow ups*.
- Tate's Algorithm to compute the Special Fiber Describes (some) blow up replacements. Describes geometrically new fibers (nodes, cusps, and others)

6 A Theorem

Definition 6.1 (Weierstrass Elliptic Scheme) *Suppose B is a smooth variety defined over a field of characteristic 0. Let X be a variety defined over B by Weierstrass equations. That is, for each open $U = Spec(R)$ of B, X is defined as the projectivization of the subscheme of $Spec(R[x, y])$ cut out by an equation*

$$y^2 = x^3 + a_4 x + a_6 \tag{1}$$

for some $a_4, a_6 \epsilon R$

$X \to B$ is called a Weierstrass Elliptic Scheme.

To say that X has a flat resolution is the content of the following theorem.

Theorem 6.2 (Flat Resolution) *Let X be a Weierstrass elliptic scheme over B. Then there exists a blowup $B' \to B$ and scheme $X' \to B'$ birational to X such that $X' \to B'$ is regular proper and flat.*

- Generalizes to fields of char $\neq 2, 3$.
- Generalizes to mixed characteristic.
- In Generality : Condition on Discriminant Divisor.

7 J=0 Families

$$y^2 = x^3 + c$$

- J invariant zero, 'CM' curve.
- Useful in cryptography. Over F_p $p = 1 \pmod 6$.
- How many points? Given p there are only 6 choices! Why: Calculate by substituting ck^6 for c (any k) (Gauss, Character Sums, $Q(\sqrt{-3}$, Cryps care.)
- Essential testing ground for my theorem.
- I consider for now limited types of bases B.

  B is two dimensional surface (locally spec$R$).

  Over a field of characteristic not 2 or 3.

  We start with a minimal Weierstrass equation, and

  The Discriminant Divisor's components intersect transversally.
- Then the Weierstrass Equation must take a very special form
  $$y^2 = x^3 + t_1^{e1} t_2^{e2}$$
  Where t_i are parameters in ring, $e_i \epsilon \{0, 1, 2, 3, 4, 5\}$
- Easier if one $e_i = 0$. (Néron Kodaira and Tate).
- I will draw the special fibers for these.
- Otherwise we have a 'collision' of Kodaira types.

8 Some Kodaira Types

- $y^2 = x^3 + 1$.

  A smooth elliptic curve.

  Name : I_0.

  Group : E.

- $y^2 = x^3 + t$. A cuspidal cubic.

  Name : II.

  Group : k^+.

- $y^2 = x^3 + t^2$. Three rational lines:

  Name : IV.

  Group : $k^+ \times Z/3Z$.

- $y^2 = x^3 + t^3$. A configuration of lines:

  Name : I_0^*.

  Group : $k^+ \times Z/2Z \times Z/2$.

- $y^2 = x^3 + t^4$. A configuration of lines:

  Name : IV^*.

  Group : $k^+ \times Z/3Z$

- $y^2 = x^3 + t^5$. A configuration of lines:

  Name : II^*.

  Group : k^+.

9 Higher Dimensions

- Tate's algorithm implies which blow ups to do.
- Technical Detail: non perfect fields appear.
- Naive approach to de singularize $y^2 = x^3 + t_1^{e_1} t_2^{e_2}$. Follow the blow ups of Tate once for e_1 and e_2.
- Proposition: Resulting scheme is regular unless both $t_1 = t_2 = 0$. That is called a *collision*.
- If we are lucky, it is regular *even* at $t_1 = t_2 = 0$.
- Compatible Collisions: $(1, 2)$, $(1, 3)$, $(1, 4)$, $(2, 3)$.
- To solve it: We alter our base: with Blow ups!

  <u>Blow Ups</u>

  Technical Algebraic Technique defines Scheme morphism.

  Graph of a map to Projective Space.

  Replaces schemes with less singular ones.

  Replaces point with whole curve showing tangent information.

  Variable substitution in practice : Result patches.

- Blow ups of rings with 2 parameters t_1 and t_2:
- substitute $t_1 = st_2$, and $t_1 s = t_2$.
- Graph old and new discriminant locus.

10 Reducing Collision Types

- Only work with Minimal Weierstrass Equations. Substitute $y = t^3 y$ and $x = t^2 x$ if $e_1 \geq 6$.
- Considers e_i mod 6.

Apply the base blow up to our family $y^2 = x^3 + t_1^{e_1} t_2^{e_2}$.

Patch 1: substitute $t_1 = s t_2$ to get:

$$y^2 = x^3 + s^{e_1} t_2^{e_1+e_2}$$

Patch 2: substitute $t_1 s = t_2$ to get:

$$y^2 = x^3 + t_1^{e_1+e_2} s^{e_2}$$

- Collision of type (e_1, e_2) becomes two separate Collisions: a (e_1, s), and (s, e_2) type Where $s = e_1 + e_2$ mod 6.
- If $s = 0$ mod 6, there is no collision.
- Continued such base changes remove many types.
- Follow this algorithm:
  Examine the discriminant divisor on the base.
  Note multiplicities (the e_i) and collision types.
  Reduce the collisions via blow ups described above as follows:

11 Limit the Collisions

1. Eliminate $(5,5)$ Collisions. Obtain new $(5,4)$ ones.
2. Eliminate $(5,4)$,$(5,3)$,$(5,2)$,$(5,1)$ Collisions.
3. Eliminate $(4,4)$,$(4,3)$,$(4,2)$ Collisions.
4. Keep the $(4,1)$ Collisions.
5. Eliminate $(3,3)$ Collisions.
6. Keep the $(3,2)$ and $(3,1)$ Collisions.
7. Eliminate $(2,2)$ Collisions. Obtain $(4,2)$ ones.
8. Eliminate $(4,2)$ Collisions.
9. Keep the $(2,1)$ Collisions.
10. Eliminate $(1,1)$ Collisions.

- We have only $(4,1)$, $(3,2)$,$(3,1)$ and $(2,1)$ Collisions.
- These are all 'Compatible' Collisions.
- The base has many patches glued together.
- Follow Tate's Algorithm for each component.
- The resulting Scheme will be Regular.
  (and Flat, Proper, Minimal)
- Conjecture: It is also a group scheme.

12 Our New Model

- The Base Changes Above and Tate's Blow ups Create a regular model in case of $J = 0$ families.
- This proves a restrictive case of the Theorem.
- General case: High dim., Mixed char, (also 2 and 3).
- Every fiber not over Discriminant is an Elliptic curve.
- Fiber over only one component are described above.
- Fibers above compatible collisions are new types.
- Recall: Scheme is regular; Fibers have singularities.
- Removing the singular points and double lines makes even the singular fiber types into groups.
- There are relationships between group structure between fibers. When models are regular, this may apply to singular fibers, which have simpler group structure.
- This is research in progress.
- Application: Study Elliptic Group Schemes, Néron models.
- Relate group structure to simpler fiber group Structure.

13 Research on Curves

There are several benefits to considering Elliptic curves as members of families. Some pure math research topics might be:

- Compare Group Structure between fibers in the same family.
- Find curves so that $\#E$ has big prime factors.
- Rephrase Arithmetic operations in terms of Group Schemes.
- Fit desirable curves into families
- Moduli spaces with mixed characteristic
- How can we relate the group structure of Elliptic curves over finite fields to Finite fields themselves? (Embedding problem)

Other interesting group objects can be used to make one way functions.

- Abelian varieties: Come from higher genus curves. (E.g Hyper-elliptic).