Reductions of Elliptic Curves and Their Galois Representations

Ethan Karpeles, Department of Mathematics
Dr. Lea Beneish, Department of Mathematics, University of North Texas

Abstract

Elliptic curves can often be described by solutions to equations of the form $y^2 = x^3 + Ax + B$. Elliptic curves have several applications including the proof of Fermat's Last Theorem and elliptic curve cryptography. A natural question to ask is whether an elliptic curve defined over the rational numbers keeps the same structure when reduced modulo a prime. We construct infinite families of elliptic curves with good or semistable reduction. The goal will be to find which of these infinite families have Galois representations with maximal image for all but finitely many specializations.

Background (Weierstrass Equations)

Definition: Elliptic Curve [3]

An **elliptic curve** is a smooth curve having a specified base point with an equation of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Here $O = [0:1:0]$ and $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

Theorem: Mordell–Weil Theorem [3]

The set of points $E(\mathbb{Q})$ of an elliptic curve form a finitely generated abelian group so $E(\mathbb{Q}) \cong \mathbb{Z}^r \otimes E[\text{tors}]$ where $E[\text{tors}]$ is finite.

Definition: Weierstrass Equation [3]

Equations of the form above that define elliptic curves are called **Weierstrass Equations**.

We can rewrite these equations in non-homogeneous coordinates $x = \frac{X}{Z}, y = \frac{Y}{Z}$:

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

We define the following values:

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

Definition: Discriminant [3]

The quantity Δ is called the **discriminant** of the Weierstrass equation.

Suppose that we have a curve defined by the Weierstrass equation:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

Definition: Singular Points [3]

A point P on this curve is said to be **singular** if and only if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$.

Definition: Nodes and Cusps [3]

A singular point P on f is a **node** if it has two tangent lines. In contrast, a singular point P on f is a **cusp** if it has only one tangent line.

Our elliptic curves are isomorphic to Weierstrass equations of the form:

$$E\colon y^2 = x^3 + Ax + B$$

Associated to this equation is the quantity $\Delta = -16(4A^3 + 27B^2)$. [3]

Background (Good and Bad Reduction)

Definition: The p-adic Valuation, Numbers, and Integers [2]

The **p-adic valuation** on $\mathbb{Q}$ is defined by a function $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Let $x \in \mathbb{Q}$ where $x \neq 0$. If $x \in \mathbb{Z}\backslash\{0\}$, let $v_p(x)$ be the unique positive integer satisfying:

$$x = p^{v_p(x)}x', \text{ where } p \nmid x'$$

For all nonzero $x \in \mathbb{Q}$, we may write $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}$. Then we define:

$$v_p(x) = v_p(a) - v_p(b)$$

Lastly, we define $v_p(0) = +\infty$.
The **field of p-adic numbers**, $\mathbb{Q}_p$, is defined to be the completion of $\mathbb{Q}$ with respect to the p-adic valuation.
The **ring of p-adic integers**, $\mathbb{Z}_p$, is defined to be $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \text{ such that } v_p(x) \geq 0\}$.

For a prime number p, we look at the operation of "reduction modulo p", which we denote by a tilde. The natural reduction map $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ is denoted by $t \mapsto \tilde{t}$.
One can find a Weierstrass equation for $E/\mathbb{Q}_p$ where $a_i \in \mathbb{Z}_p$ and so we can reduce its coefficients modulo p to obtain a (possibly singular) curve over $\mathbb{Z}/p\mathbb{Z}$:

$$\tilde{E}\colon y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$$

Definition: Reduction [3]

The curve $\tilde{E}/(\mathbb{Z}/p\mathbb{Z})$ is called the **reduction of E modulo p**.

The equation for $\tilde{E}$ is unique up to a change of coordinates.
The curve $\tilde{E}/(\mathbb{Z}/p\mathbb{Z})$ may be singular, but in any case the set of non-singular points $\tilde{E}_{ns}(\mathbb{Z}/p\mathbb{Z})$ forms a group.
From what we know about Weierstrass equations, we know that the reduced curve $\tilde{E}$ is one of three types. We classify E according to these properties.

Definition: Good and Bad Reduction [3]

Let $E/\mathbb{Q}_p$ be an elliptic curve, and let $\tilde{E}$ be the reduction modulo $p\mathbb{Z}_p$ of a minimal Weierstrass equation of E.

- E has **good (or stable) reduction** if $\tilde{E}$ is nonsingular.
- E has **multiplicative (or semistable) reduction** if $\tilde{E}$ has a node.
- E has **additive (or unstable) reduction** if $\tilde{E}$ has a cusp.

In the second and third cases, we say E has **bad reduction**.
If E has multiplicative reduction, then the reduction is said to be **split** if the slopes of the tangent lines at the node are in $\mathbb{Z}/p\mathbb{Z}$. Otherwise, it is **nonsplit**.

The values c_4 and Δ from earlier give us a lot of information about our elliptic curve.

Proposition

Let E be an elliptic curve. Then we have that:

$$\begin{aligned} \Delta \neq 0 &\iff E \text{ is nonsingular.} \\ \Delta = 0 \text{ and } c_4 \neq 0 &\iff E \text{ has a node.} \\ \Delta = 0 = c_4 &\iff E \text{ has a cusp.} \\ v_p(\Delta) = 0 &\iff \begin{array}{l} E \text{ has good reduction} \\ \tilde{E} \text{ is nonsingular.} \end{array} \\ v_p(\Delta) > 0,\ v_p(c_4) = 0 &\iff \begin{array}{l} E \text{ has multiplicative reduction} \\ \tilde{E} \text{ has a node.} \end{array} \\ v_p(\Delta) > 0,\ v_p(c_4) > 0 &\iff \begin{array}{l} E \text{ has additive reduction} \\ \tilde{E} \text{ has a cusp.} \end{array} \end{aligned}$$

Background (Galois Representations)

The goal of Galois Representations is to study Gal$(\bar{\mathbb{Q}}/\mathbb{Q})$.

Definition: The Group of Field Automorphisms of $\bar{\mathbb{Q}}$

We call the **group of field automorphisms of $\overline{\mathbb{Q}}$**, a fixed algebraic closure of $\mathbb{Q}$, that fix $\mathbb{Q}$ the absolute Galois group of $\mathbb{Q}$ and denote it by Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$.

The absolute Galois group Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of algebraic points $E(\overline{\mathbb{Q}})$ and hence induces a homomorphism $\rho_{E,p}\colon$ Gal$(\overline{\mathbb{Q}}/\mathbb{Q}) \to$ GL$_2(\mathbb{Z}/p\mathbb{Z})$ for every prime number p.

Background (Division Polynomials)

To find the coordinates of integer multiples of a point P on an elliptic curve, we recursively construct polynomials ϕ_n, ω_n, ψ_n so that $nP = (\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3})$ as so [1]:

$$\begin{aligned} \psi_1 &= 1 & \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_2 &= 2y & \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \end{aligned}$$

$$\begin{aligned} 2y\psi_{2n} &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) & \psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \\ \phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1} & 4y\omega_n &= \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2 \end{aligned}$$

Definition: Division Polynomials [1]

The polynomials ϕ_n, ω_n, ψ_n are called **division polynomials**.

Extend these to all of $\mathbb{Z}$ by $\psi_0 = 0$, $\psi_{-n} = -\psi_n$, $\phi_n = \phi_{-n}$, and $\omega_n = \omega_{-n}$. [1]

Goal of Research

The goal of the research project is to find an infinite family of elliptic curves E_t such that for all but finitely many specializations t, $\rho_{E,p}$ is surjective for all primes p.

Results

After writing a program in Python, we were able to find hundreds of infinite families of elliptic curves with good or semistable reduction modulo every possible prime number by setting $c_4 = 1$. Among these are the following:

$$\{E : y^2 = x^3 + \tfrac{1}{4}x^2 + q \mid q \in \mathbb{Q}\} \quad \{E : y^2 + xy + y = x^3 + q \mid q \in \mathbb{Q}\}$$

A deep result of Mazur implies that for elliptic curves with semistable reduction at $p \geq 11$, the image $\rho_{E,p}$ is surjective. Therefore, the remaining tasks are to understand the representations $\rho_{E,p}$ for $p < 11$. We will do this by analyzing the division polynomials of the family and studying their factorizations.

Acknowledgments

I would like to extend my sincerest thank you to Dr. Lea Beneish for suggesting this problem and for guiding me throughout the research process.

References

[1] Clemens Adelmann. *The Decomposition of Primes in Torsion Point Fields*. Springer, 2001.

[2] Alexa Pomerantz. *An Introduction To The p-Adic Numbers*. 2020.

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2016.