Elliptic Curves and the abc Conjecture

Anton Hilado

University of Vermont

October 16, 2018
Overview

1. The abc conjecture
2. Elliptic Curves
3. Reduction of Elliptic Curves and Important Quantities Associated to Elliptic Curves
4. Szpiro’s Conjecture
The Radical

Definition

The **radical** $\text{rad}(N)$ of an integer $N$ is the product of all distinct primes dividing $N$

$$\text{rad}(N) = \prod_{p|N} p.$$
The Radical - An Example

\[
\text{rad}(100) = \text{rad}(2^2 \cdot 5^2) = 2 \cdot 5 = 10
\]
The abc Conjecture

Conjecture (Oesterle-Masser)

Let $\epsilon > 0$ be a positive real number. Then there is a constant $C(\epsilon)$ such that, for any triple $a, b, c$ of coprime positive integers with $a + b = c$, the inequality

$$c \leq C(\epsilon) \text{rad}(abc)^{1+\epsilon}$$

holds.
The abc Conjecture - An Example

\[ 2^{10} + 3^{10} = 13 \cdot 4621 \]
Fermat’s Last Theorem

There are no integers satisfying

\[ x^n + y^n = z^n \text{ and } xyz \neq 0 \]

for \( n > 2 \).
Fermat’s Last Theorem - History

- $n = 4$ by Fermat (1670)
- $n = 3$ by Euler (1770 - gap in the proof), Kausler (1802), Legendre (1823)
- $n = 5$ by Dirichlet (1825)
- Full proof proceeded in several stages:
  - Taniyama-Shimura-Weil (1955)
  - Hellegouarch (1976)
  - Frey (1984)
  - Serre (1987)
  - Ribet (1986/1990)
  - Wiles (1994)
  - Wiles-Taylor (1995)
The abc Conjecture Implies (Asymptotic) Fermat’s Last Theorem

Assume the abc conjecture is true and suppose $x$, $y$, and $z$ are three coprime positive integers satisfying

$$x^n + y^n = z^n.$$

Let $a = x^n$, $b = y^n$, $c = z^n$, and take $\epsilon = 1$. Since $abc = (xyz)^n$ the statement of the abc conjecture gives us

$$z^n \leq C(\epsilon) \text{rad}((xyz)^n)^2 = C(\epsilon) \text{rad}(xyz)^2 \leq C(\epsilon)(xyz)^2 < C(\epsilon)z^6.$$

Hence there are only finitely many $z$ that satisfy the equation for $n \geq 6$. If, in addition, we can take $C(\epsilon)$ to be 1, then the abc conjecture implies Fermat’s Last Theorem, since it has been proven classically for $n < 6$. 
An **abelian variety** is a projective variety which is an abelian group object in the category of varieties.

An **elliptic curve** is an abelian variety of dimension 1.
Every elliptic curve $E$ over a field $K$ can be written as a cubic of the following form in $\mathbb{P}^2_K$:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2XZ^2 + a_4X^2Z + a_6Z^3.$$ 

Such a cubic is called a **Weierstrass equation**.
The Affine Weierstrass Equation of an Elliptic Curve over $K$

Equation in $\mathbb{P}^2$ (projective Weierstrass equation):

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2XZ^2 + a_4X^2Z + a_6Z^3.$$ 

Equation in $(\mathbb{P}^2 \setminus \{Z = 0\}) = \mathbb{A}^2$ (affine Weierstrass equation):

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

Conversion:

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}.$$
Admissible Changes of Coordinates

Let \( u, r, s, t \in K \), \( u \neq 0 \),

\[
X' = u^2 X + r
\]
\[
Y' = u^3 Y + u^2 sX + t
\]
\[
Z' = Z
\]
Short Weierstrass Form

If $\text{char}(K) \neq 2, 3$, we can use the admissible changes of coordinates to write any elliptic curve in **short Weierstrass form**:

$$y^2 = x^3 + Ax + B$$
Let $C$ be a curve in $\mathbb{P}^2_K$ given by the homogeneous equation

$$F(X, Y, Z) = 0.$$ 

Then a **singular point** on $C$ is a point with coordinates $a$, $b$, and $c$ such that

$$\frac{\partial F}{\partial X}(a, b, c) = \frac{\partial F}{\partial Y}(a, b, c) = \frac{\partial F}{\partial Z}(a, b, c) = 0.$$ 

If $C$ has no singular points, it is called **nonsingular**.
If there is only one tangent line through a singular point, it is called a cusp.

Figure: The curve $y^2 = x^3$ has a cusp at $(0, 0)$. 
If there are two distinct tangent lines through a singular point, it is called a node.

Figure: The curve $y^2 = x^3 - 3x + 2$ has a node at $(1, 0)$. 
More accurately, a point $p$ on some variety $X$ is called a singular point if $\dim(\mathfrak{m}/\mathfrak{m}^2) \neq \dim(X)$, where $\mathfrak{m}$ is the unique maximal ideal of the stalk of the structure sheaf at $p$. 
A Weierstrass equation with coefficients in \( K \) can be made into a Weierstrass equation with coefficients in the ring of integers \( \mathcal{O}_K \) by "clearing denominators". We can then \textbf{reduce} the coefficients modulo a prime ideal \( p \) to obtain a Weierstrass equation with coefficients in some finite field \( \mathbb{F}_q \).
Given a variety $X$ over $K$, a model $\mathcal{X}$ for $X$ is a scheme over $\mathcal{O}_K$ such that $X$ is isomorphic to its generic fiber.
If an elliptic curve has an integral Weierstrass equation that remains nonsingular after reduction mod $p$, we say that $p$ is a prime of **good reduction**. Otherwise, we say that it has **bad reduction**.
Kinds of Bad Reduction

We have the following kinds of bad reduction depending on the type of singular point we obtain after reduction mod $p$:

- If it is a **cusp**, we say that $p$ is a prime of **additive reduction**.
- If it is a **node**, we say that $p$ is a prime of **multiplicative reduction**. If, in addition, the slopes of the tangent lines are given by rational numbers, we say that $p$ is a prime of **split multiplicative reduction**.
Let $E$ be an elliptic curve with Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2XZ^2 + a_4X^2Z + a_6Z^3.$$ 

The **discriminant** of an elliptic curve is defined to be the quantity

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6 + 9b_2 b_4 b_6$$

where

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = a_1 a_3 + 2a_4$$
$$b_6 = a_2^2 + 4a_6$$
$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$
If we can express $E$ in short Weierstrass form as follows,

$$y^2 = f(x)$$

where $f(x)$ is some cubic polynomial, the discriminant is just the discriminant of $f(x)$. 
The local minimal discriminant of an elliptic curve $E$ over $K_p$ is defined to be the discriminant of the Weierstrass equation for which $\text{ord}_p(\Delta)$ is minimal. 

The global minimal discriminant of an elliptic curve over $K$ is defined to be

$$\Delta = \prod_p p^{\text{ord}_p(\Delta_p)}$$

where $\Delta_p$ is the discriminant of the Weierstrass equation of $E$ over $K_p$. 

A Weierstrass equation is minimal if its discriminant is the same as the minimal discriminant. The following conditions imply that a Weierstrass equation is minimal:

\[ \text{ord}_p(\Delta) < 12 \]

or

\[ \text{ord}_p(c_4) < 4 \]

or

\[ \text{ord}_p(c_6) < 6 \]

where

\[ c_4 = b_2^2 - 24b_4 \]

and

\[ c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \]
If the minimal discriminant $\Delta$ of a curve is zero, then the curve is singular (and therefore not an elliptic curve). Therefore a prime $p$ is a prime of bad reduction if and only if $p|\Delta$. 
If the discriminant of a Weierstrass equation over a global field $K$ is the same as its minimal discriminant, we say that it is a global minimal Weierstrass equation.
If $K$ has class number one, then every elliptic curve $E_K$ has a global minimal Weierstrass equation.
The conductor of an elliptic curve is defined to be the quantity

$$C = \prod_p p^{f_p}$$

where

- $f_p = 0$ if $p$ is a prime of **good reduction**.
- $f_p = 1$ if $p$ is a prime of **multiplicative reduction**.
- $f_p \geq 2$ if $p$ is a prime of **additive reduction**.
Szpiro’s Conjecture

For every elliptic curve $E$ over $\mathbb{Q}$, and every $\epsilon > 0$, there is a constant $c(E, \epsilon)$ such that

$$|\Delta| < c(E, \epsilon)(C^{6+\epsilon})$$
The Frey Curve

Definition

The Frey curve is the elliptic curve given by the affine Weierstrass equation

\[ y^2 = x(x - a)(x + b). \]
Let $E$ be the Frey curve. We either have

$$\left| \Delta \right| = 2^4 (abc)^2$$

or

$$\left| \Delta \right| = 2^{-8} (abc)^2$$
The Frey curve has multiplicative reduction at all odd primes that divide the discriminant. Therefore

\[ C = 2^{f_p} \prod_{\substack{p|abc \\ p \neq 2}} p \]

where \(2^{f_p}|\Delta\). 
Szpiro’s Conjecture Implies the abc Conjecture

\[ |\Delta| = < c(E, \epsilon)(C^{6+\epsilon}) \]
\[ 2^{-8}(abc)^2 \leq c(E, \epsilon)2^{f_p} \left( \prod_{\substack{p|abc \quad p \neq 2}} p \right)^{6+\epsilon} \]
\[ 2^{-8}(abc)^2 \leq c(E, \epsilon)2^{12+2\epsilon} \left( \prod_{\substack{p|abc \quad p \neq 2}} p \right)^{6+\epsilon} \]
\[ (c)^4 \leq c(E, \epsilon)(\text{rad}(abc))^{6+\epsilon} \]
\[ (c) \leq c(E, \epsilon)(\text{rad}(abc))^{\frac{3}{2}+\epsilon} \]
References

Enrico Bombieri and Walter Gubler (2006)
Heights in Diophantine Geometry

Joseph Silverman (2009)
The Arithmetic of Elliptic Curves

Joseph Silverman (1994)
Advanced Topics in the Arithmetic of Elliptic Curves

Serge Lang (1991)
Number Theory III
The End