Modern Number Theory: Rank of Elliptic Curves

Sunil Chetty

Department of Mathematics
University of California, Irvine

October 24, 2007

Outline

Introduction

The modern development of the theory of elliptic curves has been guided by two major questions.

Modularity

Is every elliptic curve modular?

Rank

What natural numbers can occur as the rank of an elliptic curve and is this rank effectively computable?

We are concerned with this second question and the conjectures which arise from it. One should note that there is some overlap with these two questions and their associated theories.

General Curves

- For a general curve C, a basic question is to determine the rational points on C. The *genus* g_C of the curve turns out to be an important invariant.

(1983) Faltings proved that if $g_C \geq 2$ then $C(\mathbb{Q})$ is finite.

(1890) Hilbert and Hurwitz showed that if $g_C = 0$ then the issue reduces to linear and quadratic equations. Moreover, in the latter case they showed that $C(\mathbb{Q})$ is non-empty if and only if C has p-adic points for all p, and in turn $C(\mathbb{Q})$ non-empty implies that there are infinitely many rational points.

Definitions

An elliptic curve E is:

- The non-singular solution-set of a Weierstrass equation

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

- Smooth projective algebraic curve of genus 1 with a defined point O_E.
- One dimensional abelian variety.
- A compact Riemann surface (over $\mathbb{C}$) of genus 1.

When the defining Weierstrass equation has coefficients in K and $O_E \in E(K)$, we say that E is defined over K, denoted E/K.

Definitions

An elliptic curve E is:

- The non-singular solution-set of a Weierstrass equation

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

- Smooth projective algebraic curve of genus 1 with a defined point O_E.
- One dimensional abelian variety.
- A compact Riemann surface (over $\mathbb{C}$) of genus 1.

When the defining Weierstrass equation has coefficients in K and $O_E \in E(K)$, we say that E is defined over K, denoted E/K.

Definitions

An elliptic curve E is:

- The non-singular solution-set of a Weierstrass equation

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

- Smooth projective algebraic curve of genus 1 with a defined point O_E.
- One dimensional abelian variety.
- A compact Riemann surface (over $\mathbb{C}$) of genus 1.

When the defining Weierstrass equation has coefficients in K and $O_E \in E(K)$, we say that E is defined over K, denoted E/K.

Simplified

- If $\mathrm{char}(K) \neq 2, 3$, a general Weiestrass equation can be transformed to a simpler (affine) equation $y^2 = x^3 + ax + b$. $E(K) \setminus \{O_E\}$ is then $\left\{(x, y) \in K^2 : \ y^2 = x^3 + ax + b\right\}$
- The point at infinity has (projective) coordinates $O_E = [0 : 1 : 0]$ and so for $a, b \in \mathbb{Q}$ the curve $y^2 = x^3 + ax + b$ is defined over $\mathbb{Q}$.
- $\mathbb{Q}[E] = \mathbb{Q}[x, y]/(y^2 - x^3 - ax - b) = \mathbb{Q}[x, \sqrt{x^3 + ax + b}]$ implies

$$\mathbb{Q}(E) = \mathrm{Frac}(\mathbb{Q}[E]) = \mathbb{Q}(x, \sqrt{x^3 + ax + b})$$

which has transcendental degree 1 over $\mathbb{Q}(x)$.

Simplified

- If $\mathrm{char}(K) \neq 2, 3$, a general Weiestrass equation can be transformed to a simpler (affine) equation $y^2 = x^3 + ax + b$. $E(K) \setminus \{O_E\}$ is then $\left\{(x, y) \in K^2 : \ y^2 = x^3 + ax + b\right\}$
- The point at infinity has (projective) coordinates $O_E = [0 : 1 : 0]$ and so for $a, b \in \mathbb{Q}$ the curve $y^2 = x^3 + ax + b$ is defined over $\mathbb{Q}$.
- $\mathbb{Q}[E] = \mathbb{Q}[x, y]/(y^2 - x^3 - ax - b) = \mathbb{Q}[x, \sqrt{x^3 + ax + b}]$ implies

$$\mathbb{Q}(E) = \mathrm{Frac}(\mathbb{Q}[E]) = \mathbb{Q}(x, \sqrt{x^3 + ax + b})$$

which has transcendental degree 1 over $\mathbb{Q}(x)$.

Simplified

- If $\mathrm{char}(K) \neq 2, 3$, a general Weiestrass equation can be transformed to a simpler (affine) equation $y^2 = x^3 + ax + b$. $E(K) \setminus \{O_E\}$ is then $\left\{(x, y) \in K^2 : \ y^2 = x^3 + ax + b\right\}$
- The point at infinity has (projective) coordinates $O_E = [0 : 1 : 0]$ and so for $a, b \in \mathbb{Q}$ the curve $y^2 = x^3 + ax + b$ is defined over $\mathbb{Q}$.
- $\mathbb{Q}[E] = \mathbb{Q}[x, y]/(y^2 - x^3 - ax - b) = \mathbb{Q}[x, \sqrt{x^3 + ax + b}]$ implies

$$\mathbb{Q}(E) = \mathrm{Frac}(\mathbb{Q}[E]) = \mathbb{Q}(x, \sqrt{x^3 + ax + b})$$

which has transcendental degree 1 over $\mathbb{Q}(x)$.

Examples

- Is $C_1(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + x^2\}$ an elliptic curve?
  No. Notice that the point $(0, 0)$ satisfies both partial derivatives of $f(x, y) = y^2 - x^3 - x^2$ simultaneously, i.e. it is a singular point.

- Is $C_2(K) = \{(x, y) \in K^2 : \ y^2 = x^3 + 1\}$ an elliptic curve?
  Not always. If $\text{char}(K) = 2$ then the point $(0, 1)$ is singular. If $\text{char}(K) = 3$ then the point $(-1, 0)$ is singular.

- $E : \ y^2 = x^3 - x$ is an elliptic curve defined over $\mathbb{Q}$. The points $(0, 0), (1, 0), (-1, 0) \in \mathbb{Q}^2$ satisfy the equation, so we know that $E(\mathbb{Q}) \neq \{O_E\}$. The question then becomes, are these all the points of $E(\mathbb{Q})$?

Examples

- Is $C_1(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + x^2\}$ an elliptic curve? No. Notice that the point $(0, 0)$ satisfies both partial derivatives of $f(x, y) = y^2 - x^3 - x^2$ simultaneously, i.e. it is a singular point.

- Is $C_2(K) = \{(x, y) \in K^2 : \ y^2 = x^3 + 1\}$ an elliptic curve? Not always. If $\text{char}(K) = 2$ then the point $(0, 1)$ is singular. If $\text{char}(K) = 3$ then the point $(-1, 0)$ is singular.

- $E : \ y^2 = x^3 - x$ is an elliptic curve defined over $\mathbb{Q}$. The points $(0, 0), (1, 0), (-1, 0) \in \mathbb{Q}^2$ satisfy the equation, so we know that $E(\mathbb{Q}) \neq \{O_E\}$. The question then becomes, are these all the points of $E(\mathbb{Q})$?

Examples

- Is $C_1(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + x^2\}$ an elliptic curve? No. Notice that the point $(0, 0)$ satisfies both partial derivatives of $f(x, y) = y^2 - x^3 - x^2$ simultaneously, i.e. it is a singular point.

- Is $C_2(K) = \{(x, y) \in K^2 : \ y^2 = x^3 + 1\}$ an elliptic curve? Not always. If $\text{char}(K) = 2$ then the point $(0, 1)$ is singular. If $\text{char}(K) = 3$ then the point $(-1, 0)$ is singular.

- $E : \ y^2 = x^3 - x$ is an elliptic curve defined over $\mathbb{Q}$. The points $(0, 0), (1, 0), (-1, 0) \in \mathbb{Q}^2$ satisfy the equation, so we know that $E(\mathbb{Q}) \neq \{O_E\}$. The question then becomes, are these all the points of $E(\mathbb{Q})$?

Examples

- Is $C_1(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + x^2\}$ an elliptic curve? No. Notice that the point $(0, 0)$ satisfies both partial derivatives of $f(x, y) = y^2 - x^3 - x^2$ simultaneously, i.e. it is a singular point.

- Is $C_2(K) = \{(x, y) \in K^2 : \ y^2 = x^3 + 1\}$ an elliptic curve? Not always. If $\text{char}(K) = 2$ then the point $(0, 1)$ is singular. If $\text{char}(K) = 3$ then the point $(-1, 0)$ is singular.

- $E : \ y^2 = x^3 - x$ is an elliptic curve defined over $\mathbb{Q}$. The points $(0, 0), (1, 0), (-1, 0) \in \mathbb{Q}^2$ satisfy the equation, so we know that $E(\mathbb{Q}) \neq \{O_E\}$. The question then becomes, are these all the points of $E(\mathbb{Q})$?

Examples

- Is $C_1(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + x^2\}$ an elliptic curve? No. Notice that the point $(0, 0)$ satisfies both partial derivatives of $f(x, y) = y^2 - x^3 - x^2$ simultaneously, i.e. it is a singular point.

- Is $C_2(K) = \{(x, y) \in K^2 : \ y^2 = x^3 + 1\}$ an elliptic curve? Not always. If $\text{char}(K) = 2$ then the point $(0, 1)$ is singular. If $\text{char}(K) = 3$ then the point $(-1, 0)$ is singular.

- $E : \ y^2 = x^3 - x$ is an elliptic curve defined over $\mathbb{Q}$. The points $(0, 0), (1, 0), (-1, 0) \in \mathbb{Q}^2$ satisfy the equation, so we know that $E(\mathbb{Q}) \neq \{O_E\}$. The question then becomes, are these all the points of $E(\mathbb{Q})$?

Group Structure

There is a natural (abelian) group structure on an elliptic curve.

- Geometrically: Three collinear points sum to zero (O_E).
- Algebraically: Consider the curve $E: \ y^2 = x^3 + ax + b$
  - If $x_1 = x_2$, $y_1 = -y_2$ then $(x_1, y_1) + (x_2, y_2) = O_E$
  - Otherwise

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

with

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ or } \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

depeding on $(x_1, y_1) = (x_2, y_2)$ or not.

Thus, E is an algebraic group, and $E(K)$ is called the Mordell-Weil group of E over K.

Group Structure

There is a natural (abelian) group structure on an elliptic curve.

- Geometrically: Three collinear points sum to zero (O_E).
- Algebraically: Consider the curve $E: \ y^2 = x^3 + ax + b$
  - If $x_1 = x_2$, $y_1 = -y_2$ then $(x_1, y_1) + (x_2, y_2) = O_E$
  - Otherwise

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

with

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ or } \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

depeding on $(x_1, y_1) = (x_2, y_2)$ or not.

Thus, E is an algebraic group, and $E(K)$ is called the Mordell-Weil group of E over K.

Group Structure

There is a natural (abelian) group structure on an elliptic curve.

- Geometrically: Three collinear points sum to zero (O_E).
- Algebraically: Consider the curve $E: \ y^2 = x^3 + ax + b$
  - If $x_1 = x_2$, $y_1 = -y_2$ then $(x_1, y_1) + (x_2, y_2) = O_E$
  - Otherwise

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

with

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ or } \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

depeding on $(x_1, y_1) = (x_2, y_2)$ or not.

Thus, E is an algebraic group, and $E(K)$ is called the Mordell-Weil group of E over K.

Rank

Mordell-Weil Theorem

Let K be a number field and E an elliptic curve defined over K. The Mordell-Weil group $E(K)$ is finitely generated.

Thus, we can decompose $E(K)$ as

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r.$$

- $E_{tors}(K)$ is the set of points defined over K of finite order.
- The quantity r is called the *rank* of E.
- Currently, there is no known algorithm to compute rank.

Rank

Mordell-Weil Theorem

Let K be a number field and E an elliptic curve defined over K. The Mordell-Weil group $E(K)$ is finitely generated.

Thus, we can decompose $E(K)$ as

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r.$$

- $E_{tors}(K)$ is the set of points defined over K of finite order.
- The quantity r is called the *rank* of E.
- Currently, there is no known algorithm to compute rank.

Rank

Mordell-Weil Theorem

Let K be a number field and E an elliptic curve defined over K. The Mordell-Weil group $E(K)$ is finitely generated.

Thus, we can decompose $E(K)$ as

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r.$$

- $E_{tors}(K)$ is the set of points defined over K of finite order.
- The quantity r is called the *rank* of E.
- Currently, there is no known algorithm to compute rank.

Triangles

Consider a right triangle with sides X, Y, and Z, and further assume that $X < Y < Z$. We shall call a rational number r a *congruent number* if it is the area of such a triangle with rational sides.

Question

Is every rational number r a congruent number?

We can simplify this question by noticing that any rational number r which is congruent gives rise to a squarefree natural number which is also congruent. In other words congruence of r is dependent only on $r(\mathbb{Q}^+)^2$, and $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ has a unique squarefree integer in each coset.

Triangles

Consider a right triangle with sides X, Y, and Z, and further assume that $X < Y < Z$. We shall call a rational number r a *congruent number* if it is the area of such a triangle with rational sides.

Question

Is every rational number r a congruent number?

We can simplify this question by noticing that any rational number r which is congruent gives rise to a squarefree natural number which is also congruent. In other words congruence of r is dependent only on $r(\mathbb{Q}^+)^2$, and $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ has a unique squarefree integer in each coset.

Some Algebra

Proposition 1

There is a bijection between triangles with sides X, Y, Z and area n and rational numbers x such that $x + n$ and $x - n$ are rational squares.

- The maps are given by

$$\begin{aligned} (X, Y, Z) &\mapsto \quad x = (Z/2)^2 \\ x &\mapsto \quad (\sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n},\ 2\sqrt{\alpha}) \end{aligned}$$

- From the equations $X^2 + Y^2 = Z^2$, $\frac{1}{2}XY = n$ one obtains $(X \pm Y)^2 = Z^2 \pm 4n$.

A Curve

- The equations $(X \pm Y)^2 = Z^2 \pm 4n$ multiplied together give
$$((X^2 - Y^2)/4)^2 = (Z/2)^4 - n^2.$$
- Rewriting this, we have $u^4 - n^2 = v^2$ and multiplying again by u^2, we obtain $u^6 - n^2u^2 = (uv)^2$.
- Define $E_n : \ y^2 = x^3 - n^2x$. We have a relationship between $E_n(\mathbb{Q})$ and congruent numbers.

Proposition 2

Let $(x, y) \in E_n(\mathbb{Q})$ such that $x \in (\mathbb{Q}^+)^2$, x has even denominator, and the numerator of x is prime to n. Then there exists a triangle with rational sides and area n via the map in Proposition 1.

A Curve

- The equations $(X \pm Y)^2 = Z^2 \pm 4n$ multiplied together give
$$((X^2 - Y^2)/4)^2 = (Z/2)^4 - n^2.$$
- Rewriting this, we have $u^4 - n^2 = v^2$ and multiplying again by u^2, we obtain $u^6 - n^2u^2 = (uv)^2$.
- Define $E_n : \ y^2 = x^3 - n^2x$. We have a relationship between $E_n(\mathbb{Q})$ and congruent numbers.

Proposition 2

Let $(x, y) \in E_n(\mathbb{Q})$ such that $x \in (\mathbb{Q}^+)^2$, x has even denominator, and the numerator of x is prime to n. Then there exists a triangle with rational sides and area n via the map in Proposition 1.

Rank

Lemma 3

The torsion subgroup of $E_n(\mathbb{Q})$ is $E_n(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

- There are maps $E_n(\mathbb{Q}) \to E_n(\mathbb{F}_p)$ which are injective for most p, and $\#E_n(\mathbb{F}_p) = p + 1$ for $p \equiv 3 \pmod 4$.

Proposition 4

n is a congruent number if and only if $E_n(\mathbb{Q})$ has nonzero rank.

($\Rightarrow$) The non-trivial 2-torsion points have first coordinate $x \in \{0, \pm n\}$ and Prop 2 gives a point with first coordinate $x \in (\mathbb{Q}^+)^2$. Therefore Lemma 3 guarantees a point of infinite order.

($\Leftarrow$) If P has infinite order then $x(2P)$ satisfies the hypotheses of Prop 2.

Rank

Lemma 3

The torsion subgroup of $E_n(\mathbb{Q})$ is $E_n(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

- There are maps $E_n(\mathbb{Q}) \to E_n(\mathbb{F}_p)$ which are injective for most p, and $\#E_n(\mathbb{F}_p) = p + 1$ for $p \equiv 3 \pmod 4$.

Proposition 4

n is a congruent number if and only if $E_n(\mathbb{Q})$ has nonzero rank.

($\Rightarrow$) The non-trivial 2-torsion points have first coordinate $x \in \{0, \pm n\}$ and Prop 2 gives a point with first coordinate $x \in (\mathbb{Q}^+)^2$. Therefore Lemma 3 guarantees a point of infinite order.

($\Leftarrow$) If P has infinite order then $x(2P)$ satisfies the hypotheses of Prop 2.

L-function

Consider a number field K and a prime υ. One defines $L_\upsilon(q_\upsilon^{-s})$ by G_K action on $T_\ell(E) = \varprojlim E[\ell^n]$.

- For a prime υ not dividing ℓ, from local field theory $D_\upsilon/I_\upsilon \cong \mathrm{Gal}(K_\upsilon^{\mathrm{ur}}/K_\upsilon)$ is generated by the Frobenius map $\mathrm{Frob}_{q_\upsilon}$.
- The Euler factor $L_\upsilon(q_\upsilon^{-s})$ is then

$$L_\upsilon(q_\upsilon^{-s}) = \det(1 - q_\upsilon^{-s}\mathrm{Frob}_{q_\upsilon} \,|\, T_\ell(E)^{I_\upsilon})^{-1}.$$

Definition

The global L-function of E/K is defined by the Euler product $L(E/K, s) = \prod_\upsilon L_\upsilon(q_\upsilon^{-s})$

Standard Conjectures

Analytic Continuation conjecture

The L-function $L(E/K, s)$ has an analytic continuation to the entire complex plane.

As a consequence of the work of Wiles, Breuil, Conrad, Diamond, and Taylor, the modularity question has been answered over $\mathbb{Q}$, which proves this conjecture over $\mathbb{Q}$.

Functional Equation conjecture

$L^*(s) = N_E^{(s/2)}(2\pi)^{-s}\Gamma(s)L(E/K, s)$ satisfies a functional equation

$$L^*(s) = \pm L^*(2 - s).$$

Standard Conjectures

Analytic Continuation conjecture

The L-function $L(E/K, s)$ has an analytic continuation to the entire complex plane.

As a consequence of the work of Wiles, Breuil, Conrad, Diamond, and Taylor, the modularity question has been answered over $\mathbb{Q}$, which proves this conjecture over $\mathbb{Q}$.

Functional Equation conjecture

$L^*(s) = N_E^{(s/2)}(2\pi)^{-s}\Gamma(s)L(E/K, s)$ satisfies a functional equation

$$L^*(s) = \pm L^*(2 - s).$$

BSD

Birch-Swinnerton-Dyer (BSD) conjecture

The L-function $L(E, s)$ has a zero at $s = 1$ with order equal to the rank r of E and

$$\lim_{s \to 1} L(E, s)(s-1)^{-r} \sim \Omega(E) \cdot R(E) \cdot |Ш(E)|$$

(1977) Coates and Wiles prove that for CM elliptic curves, $E(\mathbb{Q})$ infinite implies $L(E/\mathbb{Q}, 1) = 0$.

(1986) Gross and Zagier prove that if $E/\mathbb{Q}$ is modular and $L(E/\mathbb{Q}, s)$ has a simple zero at $s = 1$ then $E(\mathbb{Q})$ is infinite.

(1987) Rubin proves that for CM elliptic curves $|Ш(E/\mathbb{Q})| < \infty$ and if $r \geq 2$ then the order of vanishing of $L(E/\mathbb{Q}, 1)$ is ≥ 2.

BSD

Birch-Swinnerton-Dyer (BSD) conjecture

The L-function $L(E, s)$ has a zero at $s = 1$ with order equal to the rank r of E and

$$\lim_{s \to 1} L(E, s)(s-1)^{-r} \sim \Omega(E) \cdot R(E) \cdot |Ш(E)|$$

(1977) Coates and Wiles prove that for CM elliptic curves, $E(\mathbb{Q})$ infinite implies $L(E/\mathbb{Q}, 1) = 0$.

(1986) Gross and Zagier prove that if $E/\mathbb{Q}$ is modular and $L(E/\mathbb{Q}, s)$ has a simple zero at $s = 1$ then $E(\mathbb{Q})$ is infinite.

(1987) Rubin proves that for CM elliptic curves $|Ш(E/\mathbb{Q})| < \infty$ and if $r \geq 2$ then the order of vanishing of $L(E/\mathbb{Q}, 1)$ is ≥ 2.

Module Decomposition

Let F be an abelian extension of K and let $\chi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ be a character.

- $\mathrm{Gal}(F/K)$ acts on the Mordell-Weil group $E(F)$.
- Define the χ-eigenspace of $E(F) \otimes \mathbb{C}$ to be

$$E(F)^\chi := \{P \in E(F) \otimes \mathbb{C} \mid P^\sigma = \chi(\sigma)P \quad \forall \sigma \in \mathrm{Gal}(F/K)\}.$$

- $E(F) \otimes \mathbb{C}$ decomposes as

$$E(F) \otimes \mathbb{C} = \oplus_\chi E(F)^\chi.$$

L-function Decomposition

Again, let F be an abelian extension of K and $\chi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ a character.

- Denote $L(E/K, \chi, s)$ to be a twist of the L-function by the character χ. More precisely, in the definition of $L_\upsilon(q_\upsilon^{-s})$, one incorporates the action of χ

$$L_\upsilon(q_\upsilon^{-s}) = \det(1 - q_\upsilon^{-s}\mathrm{Frob}_{q_\upsilon} | T_\ell(E)(\chi)^{I_\upsilon})^{-1}$$

  where $T_\ell(E)(\chi)$ is the same Tate module $T_\ell(E)$ but with the action of G_K twisted by χ.

- The L-function (over F) then decomposes

$$L(E/F, s) = \prod_\chi L(E/K, \chi, s).$$

L-function Decomposition

Again, let F be an abelian extension of K and $\chi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ a character.

- Denote $L(E/K, \chi, s)$ to be a twist of the L-function by the character χ. More precisely, in the definition of $L_\upsilon(q_\upsilon^{-s})$, one incorporates the action of χ

$$L_\upsilon(q_\upsilon^{-s}) = \det(1 - q_\upsilon^{-s}\mathrm{Frob}_{q_\upsilon} | T_\ell(E)(\chi)^{I_\upsilon})^{-1}$$

  where $T_\ell(E)(\chi)$ is the same Tate module $T_\ell(E)$ but with the action of G_K twisted by χ.
- The L-function (over F) then decomposes

$$L(E/F, s) = \prod_\chi L(E/K, \chi, s).$$

Modified Conjectures

Functional Equation conjecture

The L-function $L(E/K, \chi, s)$ satisfies a functional equation

$$L(E/K, \chi, s) = W(E, \chi)L(E/K, \overline{\chi}, 2 - s)$$

with $W(E, \chi) = \prod_v W_v(E, \chi)$ and $|W(E, \chi)| = 1$.

BSD conjecture

The twisted L-function $L(E, \chi, s)$ has a zero at $s = 1$ with order equal to the rank (dimension) r of E^{χ}.

Parity conjecture

If $L(E/K, \chi) = L(E/K, \overline{\chi})$, then the parity of the rank r of E^{χ} is determined by the sign of $W(E, \chi)$.

Modified Conjectures

Functional Equation conjecture

The L-function $L(E/K, \chi, s)$ satisfies a functional equation

$$L(E/K, \chi, s) = W(E, \chi)L(E/K, \overline{\chi}, 2 - s)$$

with $W(E, \chi) = \prod_v W_v(E, \chi)$ and $|W(E, \chi)| = 1$.

BSD conjecture

The twisted L-function $L(E, \chi, s)$ has a zero at $s = 1$ with order equal to the rank (dimension) r of E^{χ}.

Parity conjecture

If $L(E/K, \chi) = L(E/K, \overline{\chi})$, then the parity of the rank r of E^{χ} is determined by the sign of $W(E, \chi)$.

Modified Conjectures

Functional Equation conjecture

The L-function $L(E/K, \chi, s)$ satisfies a functional equation

$$L(E/K, \chi, s) = W(E, \chi)L(E/K, \overline{\chi}, 2 - s)$$

with $W(E, \chi) = \prod_v W_v(E, \chi)$ and $|W(E, \chi)| = 1$.

BSD conjecture

The twisted L-function $L(E, \chi, s)$ has a zero at $s = 1$ with order equal to the rank (dimension) r of E^{χ}.

Parity conjecture

If $L(E/K, \chi) = L(E/K, \overline{\chi})$, then the parity of the rank r of E^{χ} is determined by the sign of $W(E, \chi)$.

The Twist A

- Let E be an elliptic curve over K.
- We consider an abelian variety A_L for each cyclic extension L of K inside F. A_L is a twist of E in the sense of Mazur-Rubin-Silverberg (2006). When $[L : K]$ is a power of p, there is a unique prime $\mathfrak{p}_L$ above p associated to L. For the remainder, we will simply write A for A_L and $\mathfrak{p}$ for $\mathfrak{p}_L$.

Proposition 4.1 (Mazur-Rubin, 2006)

There is a canonical G_K-isomorphism $A[\mathfrak{p}] \xrightarrow{\sim} E[p]$.

Via this isomorphism, one identifies

$$H^1(K_v, A[\mathfrak{p}]) \cong H^1(K_v, E[p]).$$

The Twist A

- Let E be an elliptic curve over K.
- We consider an abelian variety A_L for each cyclic extension L of K inside F. A_L is a twist of E in the sense of Mazur-Rubin-Silverberg (2006). When $[L : K]$ is a power of p, there is a unique prime $\mathfrak{p}_L$ above p associated to L. For the remainder, we will simply write A for A_L and $\mathfrak{p}$ for $\mathfrak{p}_L$.

Proposition 4.1 (Mazur-Rubin, 2006)

There is a canonical G_K-isomorphism $A[\mathfrak{p}] \xrightarrow{\sim} E[p]$.

Via this isomorphism, one identifies

$$H^1(K_v, A[\mathfrak{p}]) \cong H^1(K_v, E[p]).$$

The Twist A

- Let E be an elliptic curve over K.
- We consider an abelian variety A_L for each cyclic extension L of K inside F. A_L is a twist of E in the sense of Mazur-Rubin-Silverberg (2006). When $[L : K]$ is a power of p, there is a unique prime $\mathfrak{p}_L$ above p associated to L. For the remainder, we will simply write A for A_L and $\mathfrak{p}$ for $\mathfrak{p}_L$.

Proposition 4.1 (Mazur-Rubin, 2006)

There is a canonical G_K-isomorphism $A[\mathfrak{p}] \xrightarrow{\sim} E[p]$.

Via this isomorphism, one identifies

$$H^1(K_v, A[\mathfrak{p}]) \cong H^1(K_v, E[p]).$$

Local Selmer Conditions

- For each υ, define $H^1_{\mathcal{E}}(K_\upsilon, E[p])$ to be the image of $E(K_\upsilon)/pE(K_\upsilon)$ via

$$E(K_\upsilon)/pE(K_\upsilon) \hookrightarrow H^1(K_\upsilon, E[p]).$$

- Similarly, define $H^1_{\mathcal{A}}(K_\upsilon, E[p])$ to be the image in the composition

$$A(K_\upsilon)/\mathfrak{p}A(K_\upsilon) \hookrightarrow H^1(K_\upsilon, A[\mathfrak{p}]) \cong H^1(K_\upsilon, E[p]).$$

- Lastly, define

$$H^1_{\mathcal{E}\cap\mathcal{A}}(K_\upsilon, E[p]) := H^1_{\mathcal{E}}(K_\upsilon, E[p]) \cap H^1_{\mathcal{A}}(K_\upsilon, E[p]).$$

Defining δ_v

Definition

For each prime v of K, define the invariant $\delta_v \in \mathbb{Z}/2\mathbb{Z}$ to be

$$\begin{aligned} \delta_v &:= \dim_{\mathbb{F}_p}(H^1_{\mathcal{E}}(K_v, E[p])/H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E[p])) \pmod 2 \\ &\equiv \dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap N_{L_\omega/L'_\omega} E(L_\omega)) \pmod 2 \end{aligned}$$

The following theorem illustrates the significance of the δ_v.

Theorem 6.4 (Mazur-Rubin, 2006)

Let E/K be an elliptic curve and F an abelian extension of K. Then

$$rank_{\mathbb{Z}} E(K) - \dim_{\mathbb{C}} E(F)^{\chi} \equiv \sum_v \delta_v \pmod 2 .$$

Defining δ_v

Definition

For each prime v of K, define the invariant $\delta_v \in \mathbb{Z}/2\mathbb{Z}$ to be

$$\begin{aligned} \delta_v &:= \dim_{\mathbb{F}_p}(H^1_{\mathcal{E}}(K_v, E[p])/H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E[p])) \pmod 2 \\ &\equiv \dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap N_{L_\omega/L'_\omega} E(L_\omega)) \pmod 2 \end{aligned}$$

The following theorem illustrates the significance of the δ_v.

Theorem 6.4 (Mazur-Rubin, 2006)

Let E/K be an elliptic curve and F an abelian extension of K. Then

$$rank_{\mathbb{Z}} E(K) - \dim_{\mathbb{C}} E(F)^{\chi} \equiv \sum_v \delta_v \pmod 2 .$$

Question

Question

How do the δ_v relate to the quotients $\frac{W_v(E/K,\chi)}{W_v(E/K,1)}$?

- Mazur-Rubin show that in good reduction $\delta_v \equiv 0 \pmod 2$ and a formula of Rohrlich gives $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = 1$.
- In multiplicative reduction, the theory of Tate curves shows $\delta_v \equiv 1 \pmod 2$, and another formula of Rohrlich gives $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = -1$.
- In additive, potentially good reduction, $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = 1$; $\delta_v \equiv 0 \pmod 2$ has been shown only for the case $v \nmid p$.

Question

Question

How do the δ_v relate to the quotients $\frac{W_v(E/K,\chi)}{W_v(E/K,1)}$?

- Mazur-Rubin show that in good reduction $\delta_v \equiv 0 \pmod 2$ and a formula of Rohrlich gives $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = 1$.
- In multiplicative reduction, the theory of Tate curves shows $\delta_v \equiv 1 \pmod 2$, and another formula of Rohrlich gives $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = -1$.
- In additive, potentially good reduction, $\frac{W_v(E/K,\chi)}{W_v(E/K,1)} = 1$; $\delta_v \equiv 0 \pmod 2$ has been shown only for the case $v \nmid p$.

The End

Thanks for listening.

Referenes

- K. Ireland and M. Rosen. A Classical Introduction to Modern Number Theory. volume 87 of Graduate Texts in Mathematics. Springer, 1990.
- N. Koblitz. Introduction to Elliptic Curves and Modular Forms. volume 97 of Graduate Texts in Mathematics. Springer, 1993.
- B. Mazur and K. Rubin. Finding large selmer rank via an arithmetic theory of local constants. Annals of Mathematics 166 (2007) 581-614.
- Wiles. The Birch and Swinnerton-Dyer Conjecture. http://www.claymath.org/millennium/BirchandSwinnerton-DyerConjecture/BSD.pdf
- S-W Zhang. Elliptic Curves, L-Functions, CM-points. http://www.math.columbia.edu/szhang/papers/elc.pdf.