Elliptic Curves and Galois Representations

Caleb McWhorter

Fall 2014

General Motivation

Diophantine equations are the study of solutions of polynomial equations in integers or rationals. Take the equation $f(x, y) = 0$, we might ask:

1. Are there integer solutions?
2. Are there are rational solutions?
3. Are there infinitely many integer solutions?
4. Are there infinitely many rational solutions?

In fact, this is Hilbert's 10th Problem: Devise a process to determine in a finite number of operations whether an equation is solvable in rational integers. Only the third has been answered in full generality. In 1970, Matiyasevich, Putnam, Robinson showed no such general algorithm exists. Only the third has been fully answered and there are good partial answers for the last. For polynomials in more variables, there are only partial answers to any. The work of Davis, Matijasevič, and Robinson shows that in general it is not possible to answer the first.

An affirmative answer in one does not mean an affirmative answer for the others. For instance, the curve $y^2 = x^3 - 2$ has finitely many integral solutions but infinitely many rational solutions.

However, in some cases we can find all rational or integral solutions. A few specific instances are this are the following:

1. Linear equations in two variables: $ax + by = d$ and $ab \neq 0$ (Of course, $a, b, d \in \mathbb{Z}$). We use the Euclidean Algorithm to solve. There are always infinitely many rational solutions. However, there are integral solutions if and only if d is divisible by (a, b).
2. Polynomials in one variable: If $\frac{p}{q} \in \mathbb{Q}$ solution to $f(x) = 0$ then $p \mid a_n$ and $q \mid a_0$ (the so called Rational Roots Theorem). This gives a finite list of possible rational solutions to check.
3. Rational Conics: Legendre gives method to do this for conics via congruences though an elegant solution is given by Hasse: "A homogenous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in real numbers and in p-adic numbers for all primes p. Typically, only need be done for finitely many such points. This is for rational points. Integral points are more difficult to find, e.g. Pell's equation $x^2 - Dy^2 = 1$.

   This can also be solved with by finding a single rational point on the conic and then projecting onto an appropriate rational line. For example,

Rational Parametrization of the Circle: Project line $y = t(1+x)$ onto circle (connecting (-1,0) to point $(0,t)$ where $t \in \mathbb{Q}$). Solving yields

$$x = \cos\theta = \frac{1-t^2}{1+t^2} \qquad y = \sin\theta = \frac{2t}{1+t^2}$$

However, this assumes a rational points to start. For example, the curve $x^2 + y^2 = 3$ has no rational point to start with. To see this, view this equation mod 4.

4. Cubic equations: There exists no algorithm to yield all rational solutions. There are conjectural algorithms but none have been shown to work in full generality.

5. Higher degree: Degree ≥ 4 have genus ≥ 2 except some of degree 4 have genus 1. Mordell conjectured curve $\mathcal{C}$ of genus ≥ 2 can have only finitely many rational solutions and this proved by Faltings in 1983.

Elliptic Curve Examples

Definition (Elliptic Curve)**.** *An elliptic curve is an equation for the form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and no repeated roots.*

We begin with a few motivational examples:

Example 1 (Consecutive Perfect Squares)**.** Are there three consecutive integers whose product is a perfect square?

$$y^2 = x(x+1)(x+2) = x^3 + 3x^2 + 2x$$

▷

Example 2 (Pyramidal Arrangements)**.** Can a square arrangement of spheres be arranged into regular pyramid?

$$y^2 = 1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$$

▷

Example 3. Congruent Number Problem: A number is *congruent* if there is a rational right triangle with area n. For example, 6 is a congruent number - take a 3-4-5 triangle. Also, 5 is a congruent number take $\frac{3}{2} - \frac{20}{3} - \frac{41}{6}$. However, 1 is not a congruent number.

These can be quite complex - the congruent number 157 has a hypotenuse with 50 digits in its numerator alone. The integer 1 is not congruent by descent. Fermat showed that no perfect square can be a congruent number. Scaling a triangle changes its area by a square factor and any rational can be scaled by a suitable rational to a squarefree integer. So when considering the problem, it is sufficient to focus on squarefree positive integers.

Stephens showed in 1975 that the weak Birch and Swinnerton-Dyer conjecture implies that any positive integer $n \equiv 5, 6, 7 \mod 8$ is a congruent number. However in 1983, Tunnell discovered an enumerative criterion for congruent numbers relating to the weak Birch and Swinnerton-Dyer conjecture.

Theorem (Stephens - 1975)**.** *The weak Birch and Swinnerton-Dyer conjecture implies that any positive integer $n \equiv 5, 6, 7 \mod 8$ is a congruent number.*

Theorem (Tunnell - 1983)**.** *Let n be a squarefree positive integer. Let*

$$f(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 8z^2 = n$$
$$g(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 32z^2 = n$$
$$h(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 8z^2 = n/2$$
$$k(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 32z^2 = n/2$$

For odd n, if n is congruent then $f(n) = 2g(n)$. For even n, if n is congruent then $h(n) = 2k(n)$. Moreover, if the (weak) Birch & Swinnerton-Dyer conjecture is true for the curve $y^2 = x^3 - n^2x$ then the converse of both implications is true: $f(n) = 2g(n)$ implies n is congruent when n is odd and $h(n) = 2k(n)$ implies n is congruent when n is even.

▷

Elliptic Curves and the Chord-Tangent Law

Elliptic Curve

Definition (Elliptic Curve)**.** *An elliptic curve is an equation of the form $y^2 = x^3 + Ax + B$, where A and B are constants. This is called the Weierstrass equation for an elliptic curve. The field K will be specified. If K is a field with $L \supseteq K$ then*

$$E(K) = \{\infty\} \cup \{(x,y) \in K \times L \mid y^2 = x^3 + Ax + B\}$$

Note we do not allow multiple roots. That is, $4A^3 + 27B^2 \neq 0$. This means the curve is nonsingular (its partials do not vanish simultaneously). An elliptic curve over a field K is denoted E, $E(K)$, or $C(K)$.

For this talk, all our elliptic curves will be nonsingular and will be assumed to be elliptic curves over the field $\mathbb{Q}$ unless otherwise stated. Furthermore, though we look at a curve $E(\mathbb{Q})$, we choose $A, B \in \mathbb{Z}$.

Definition (Elliptic Curve)**.** *An elliptic curve is a projective algebraic curve of genus one with a specified rational point $\mathcal{O}$, sometimes called the point at infinity or the origin. An elliptic curve is an abelian variety.*

Here are a few examples:

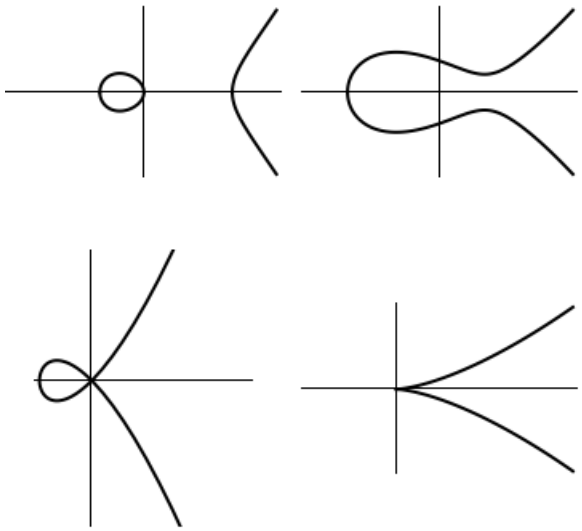

Figure 1: The elliptic curves $y^2 = x(x+1)(x+2)$,$y^2 = x^3 - 3x + 3$, $y^2 = x^2(x+1)$, and $y^2 = x^3$, respectively.

Chord-Tangent Law

The idea of a group operation is to take 2 points, operate, and obtain a third element. But a line intersects a cubic at 3 points! So if we take 2 of them we might be able to define a group by having the result be the third intersection. But what if there is none? This is why we use the projective plane!

Theorem (Bezout's Theorem)**.** *Let C_1 and C_2 be projective curves with no common components. Then*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \deg C_1 \deg C_2$$

where the sums is taken over all points of $C_1 \cap C_2$ having complex coordinates. In particular, if C_1 and C_2 are smooth curves with only transversal intersections, then $\#(C_1 \cap C_2) = \deg C_1 \deg C_2$. In all cases,

$$\#(C_1 \cap C_2) \leq \deg C_1 \deg C_2$$

Definition (Chord-Tangent Law)**.** *Start with points P, Q on an elliptic curve. Let L be the line connecting P and Q (if $P = Q$, then this is the tangent line, hence why we restrict to nonsingular elliptic curves). Then L intersects at a third point, R. Draw the line L' from R to $\mathcal{O}$. The line L' intersects E at a third point, this third point is defined to be $P + Q$.*

It is immediate that $P + Q = Q + P$. To check that $\mathcal{O}$ is the identity, draw the line L from P to $\mathcal{O}$. It intersects at a third point R. Then draw the line from R to $\mathcal{O}$, but this next point of intersection is clearly P as P, $\mathcal{O}$, and R are collinear.

To find inverses, draw the tangent line at $\mathcal{O}$ and take the third intersection to be $\mathcal{O}'$. Draw the line from $\mathcal{O}$ to P and the third intersection point E is $-P$.

Associativity can be shown with much algebra or following from the Riemann-Roch Theorem in algebraic geometry.

We often choose the origin, or point at infinity, to actually be the point at infinity. However, the choice is irrelevant:

Theorem. *The choice of origin for the chord-tangent law. The map*

$$P \mapsto P + (\mathcal{O}' - \mathcal{O})$$

is an isomorphism.

It is also important to note that the Chord-Tangent Law is invariant under birational transformations.

Points of Finite Order

Definition (Order)**.** *A point P on $C(K)$ has finite order if*

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ times}} = \mathcal{O}$$

Example 4 (Points of order 2)**.** Equivalently, these are the points $-P$. So if $P = (x, y)$, we have $-P = (x, -y)$. Then we need $y = 0$. These are the zeros of the function (the non singularity of the curve forces distinct roots). Therefore, a point $P \in C(K)$ has order two if and only if $y = 0$. Allowing complex coordinates, there are therefore 4 points of order 2: the roots of $C(K)$ and $\mathcal{O}$. They form the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. ▷

Example 5 (Points of Order 3)**.** These are the points such that $3P = \mathcal{O}$. But then $2P = -P$. With a bit of work we get that $P = (x, y)$ is a point of order 3 if and only if x is a root of the polynomial

$$\psi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$$

There are 9 points of order dividing 3. They form the group $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. ▷

Interestingly enough, the real roots of order three form a cyclic group of order 3 whereas the rational points of order 3 form either a cyclic group of order 3 or the trivial group.

Of course, due to the closure of the fields under addition/subtraction, we get the following tower of containments:

$$\{\mathcal{O}\} \subset C(\mathbb{Q}) \subset C(\mathbb{Q}) \subset C(\mathbb{R}) \subset C(\mathbb{C})$$

Whereas the methods of algebra constitute the study of $C(\mathbb{Q})$, analysis can be brought to bear to study $C(\mathbb{R})$ and $C(\mathbb{C})$.

The addition of real points on the curve is continuos. Therefore, the group $C(\mathbb{R})$ forms a 1-dimensional Lie group and is compact. If $C(\mathbb{R})$ is connected, it must be S^1. If $C(\mathbb{R})$ is not connected, then it must be $S^1 \times Z_2$.

Therefore, the points of finite order in $\mathbb{R}$ are the roots of unity. The points of order m in $C(\mathbb{R})$ form a cyclic group of order m when $C(\mathbb{R})$ is connected and when there are two connected components, if m is odd then we get a cyclic group of order m while if m is even we get a $Z_m \times Z_2$.

Moreover, the real points of order dividing 3 always form a cyclic group of order 3. There are 8 such points so that it is not possible for all the complex points of order 3 to be complex and certainly cannot all be rational.

The Structure of $C(\mathbb{C})$

Using yet another transformation, we can transform our elliptic curve into the form:

$$y^2 = 4x^3 - g_2 x - g_3$$

Since this has distinct roots, Weierstrass Theory of Elliptic Functions says that using a series of integrals one can find complex numbers ω_1, ω_2 (called *periods*). Then we form a lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$$

The choices of ω_1, ω_2 are not unique byte the lattice Λ is. We can go the other way as well: Given a lattice L, define

$$g_2 = 60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^4} \qquad g_3 = 140 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^6}$$

We use these to define the Weierstrass $\wp(u)$ function by the series

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega} \right)$$

which is a meromorphic function having poles at the points of Λ. Furthermore, it is doubly periodic. If we look at the period parallelogram, we get a 1-1 correspondence between the complex points on our elliptic curve and those inside the parallelogram (this works for any field of characteristic not 2). But then it makes finding points of finite order simple and shows that the map $\mathbb{C} \to C(\mathbb{C})$ is a homomorphism with kernel L so that $\mathbb{C}/\Lambda$ is isomorphic to $C(\mathbb{C})$. So the group of complex points over our elliptic curve is a torus: $T = \mathbb{S}^1 \times \mathbb{S}^1$. Using the lattice (specifically the period parallelogram). We see that in general the points of order m form a group of order m^2 that is $\mathbb{Z}_m \oplus \mathbb{Z}_m$.

(To be specific: we have $\mathbb{C}[x, y] = \mathbb{C}[X, Y]/(Y^2 - 4X^3 + g_2X + g_3)$ and let $\mathbb{C}[\wp, \wp']$ be the $\mathbb{C}$-algebra of meromorphic functions on $\mathbb{C}$ generated by $\wp, \wp'$. The map $(X, Y) \mapsto (\wp(z), \wp'(z))$ defines a homomorphism

$$\mathbb{C}[x, y] \to \mathbb{C}[\wp, \wp']$$

The only polynomials $g(X, Y) \in \mathbb{C}[X, Y]$ such that $g(\wp, \wp') = 0$ are those divisible by $f(X, Y) \stackrel{\text{def}}{=} Y^2 - X^3 + g_2X + g_3$. Then from $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, we obtain

$$E(\mathbb{C})_n \cong \frac{1}{n}\Lambda/\Lambda = \{\frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \mid a, b \in \mathbb{Z}\}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

which is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2. Then for any elliptic curve E over an algebraically closed field k of characteristic 0, $E(k)_n$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2.)

The Structure of $C(\mathbb{Q})$

Even $C(\mathbb{Q})$ has a "nice" structure. In fact,

Theorem (Mordell-Weil)**.** *(Conjectured Poincaré in 1908, proved Mordell in 1922, generalized in thesis by Weil in 1928): $E(\mathbb{Q})$ is a finitely generated abelian group. Hence, $E(\mathbb{Q})$ is sometimes called the Mordell-Weil group of E.*

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{torsion}$$

A fortiori, $C(\mathbb{Q})$ has finite basis.

(Note: This is really the weak Mordell-Weil Theorem. The theorem actually states that any nonsingular plane cubic curve that has a rational point has a finitely generated group of rational points. It is also conjectured that there is an algorithm to find a generating set for the Mordell-Weil group. Nevertheless, $C(\mathbb{Q})$ has finite basis.)

Theorem (Nagell-Lutz). *Let $C(\mathbb{Q})$ be a nonsingular cubic curve with integer coefficients. Then $P = (x, y) \in C(\mathbb{Q})$ has finite order then $x, y \in \mathbb{Z}$ and either $y = 0$ so that P has order 2 or y divides the discriminate of the polynomial $f(x)$ in $y^2 = f(x)$.*

Notice that the Nagell-Lutz is not an if and only if statement. This gives a finite list containing the integer torsion points (if there are any). Algorithmically, this is still a good start. We have a finite list of possibilities and we merely compute nP for $n \geq 1$ until we reach $\mathcal{O}$ or reach a point $P \in C(\mathbb{Q})$ with non-integer coordinates. But even if $P \in C(\mathbb{Q})$ has finite order, it may have very large order. What to do then? A theorem of Siegel says that there are finite number of cases to check.

Theorem (Siegel, 1929). *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then E has only a finite number of integral points. (Follows from Roth theorem on Diophantine approximation). Alan Baker found the number of such*

$$\max(|x|, |y|) < exp((10^6 \cdot \max(|A|, |B|))^{10^6})$$

(Though a better bound than Siegel's was given by Baker-Coates in 1970.) In fact, we can do much better due to a conjecture of Ogg proved by Mazur (1977/1978).

Theorem. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q})_{torsion}$ is isomorphic to one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, 3, \cdots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 4 \end{cases}$$

each one of these cases can occur (and each infinitely many). So if P is a point of order at least 13, then it must have infinite order then $E(\mathbb{Q})$ contains an infinite amount of distinct rational points. Examples:

Curve	Torsion	Generators
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(2,0)}{(0,0)}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(3,6)}{(0,0)}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(-3,18)}{(2,-2)}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(30,-90)}{(-40,400)}$

Figure 2: A table of elliptic curves of given torsion subgroup.

Billings and Mahler showed in 1940 that no elliptic curve has a torsion element with order 11. This completes the torsion part. But what of the rank? What does it "look like"? How big can the rank r be?

Proposition (Rank Conjecture). *Let $N \geq 0$ be natural. Then there exists an elliptic curve E defined over $\mathbb{Q}$ with rank $r \geq N$. Largest known rank is 28 discovered by Elkies in 2006 with trivial torsion.*

But this still leaves the issue of computing the rank or at least bounding the rank.

Galois Representations

Fermat's Last Theorem

As a brief aside,

If E is an elliptic curve over K with an extension L and σ is an automorphism of L fixing K, if $P \in E(L)$ has order m, then $\sigma(P) = (\sigma(x), \sigma(y)) \in E(L)$ has order m.

This yields a Galois representation $\rho_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m])$ given by $\sigma \mapsto$ the induced automorphism of $E[m]$ given by $P \mapsto \sigma(P)$.

In fact, looking at $E[n]$ and $\rho_{E.m}$ yields some interesting notions.

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. $G_{\mathbb{Q}}$ is a compact totally disconnected topological group. Learning about this group is perhaps the main goal of Algebraic Number Theory. Class Field Theory describes $G_{\mathbb{Q}}^{\mathrm{ab}}$. We study the representations of $G_{\mathbb{Q}}$. But

$$\varphi : G_{\mathbb{Q}} \to \mathrm{Gl}(n, \mathbb{C})$$

are dull as they have finite image. Better is to start with some $E(\mathbb{Q})$. Then $E(\overline{Q})$ is an abelian group with action of $G_{\mathbb{Q}}$. We know how $E(\mathbb{Q})_{\mathrm{torsion}}$ looks like. Then we get an action of $G_{\mathbb{Q}}$ on $E[l^n]$ yielding representation

$$\overline{\varphi} : G_{\mathbb{Q}} \to \mathrm{GL}(2, E[l^n])$$

which piece together to give the continuous representation

$$\varphi : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}_l)$$

If we started with φ, we can reduce modulo l to get

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\varphi} & \mathrm{GL}(2, \mathbb{Z}_l) \\ & \searrow^{\overline{\varphi}} & \downarrow \\ & & \mathrm{GL}(2, \mathbb{F}_l) \end{array}$$

This shows a usefulness at looking at $E[n]$. We use this idea to help look at ranks.

Shafarevich-Tate Group

Starting with an elliptic curve E over $\mathbb{Q}$ defined by

$$y^2 = (x - n)(x - p)(x - q)$$

we can perform a series of transitions to a curve $C = C_{a,b,c}$ in the projective plane. If this curve C has a rational point, it is our curve E. If C has no rational points, it is discarded. The 2-Selmer group S_2 is defined by the (a, b, b) such that $C_{a,b,c}$ has p-adic points for all $p \leq \infty$. The standard decent procedure gives

$$\varphi : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow S_2$$

the 2-torsion in the Shafarevich-Tate group is the cokernel of this map:

$$Ш_2 = S_2/\mathrm{im}\ \varphi$$

The goal is to learn about $E(\mathbb{Q})/2E(\mathbb{Q})$ and we use S_2 to do this but $Ш_2$ is the obstruction. The possible nontriviality of $Ш_2$ eliminates the possibility of computing the rank of $E(\mathbb{Q})$. The group S_2 can be computed exactly and gives us an upper bound on the rank but one cannot tell how much of S_2 is the image of φ and how much is (a, b, c) representing elements of $Ш_2$.

$G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Shafarevich-Tate group

$$Ш = \ker\left(H^1(G, E(\overline{Q})) \to \prod_{p\leq\infty} H^1(G_p, E(\overline{Q}_p))\right)$$

The n-Selmer group

$$S_n = \ker\left(H^1(G_p, E[n]) \to \prod_{p\leq\infty} H^1(G_p, E(\overline{Q}_p))\right)$$

Giving rise to the short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S_n \to Ш[n] \to 0$$

This generalizes to the short exact sequence

$$0 \to E(H_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to S(E/H_\infty) \to Ш(E/H_\infty)(p) \to 0$$

where H_∞ is an infinite Galois extension of a number field F. This is Iwasawa Theory whose central idea is to observe that the Galois group $G(H_\infty/F)$ over F has a natural left action on $S(E/H_\infty)$ and use these Galois-module structures to study $S(E/F)$ and relate $S(E/F)$ to its L-functions.

Definition (Frey Curve)**.** *For prime p, the Frey curve is*

$$E : y^2 = x(x - a^p)(x - b^p)$$

related to

$$x^p + y^p = z^p$$

where a, b are solutions to Fermat's Last Theorem $a^p + b^p = c^p$, $abc \neq 0$ and l prime..

This curve (though first considered by Hellegouarch in 1975) was proved to be not modular by Ribet-Serre (1985/1986, [Serre's] Epsilon Conjecture).

Theorem (Taniyama-Shimura)**.** *All semistable elliptic curves over $\mathbb{Q}$ are modular.*

L-functions

Of course, we are interested in calculating the rank of an elliptic curve. Unfortunately, the methods of calculating (or even bounding it) are obstructed by the Ш group. However, there is a way around this using L-functions of an elliptic curve. This is the idea of the conjecture of Birch and Swinnerton-Dyer.

Definition (L-function)**.** *A function of the form*

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n \in \mathbb{C}$ and $s \in \mathbb{C}$. One of the most special examples is $a_n = 1$ for all n which is the Riemann Zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ prime} = \frac{1}{1 - p^{-s}}$$

Definition (Reductions)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Let $\overline{E}$ be the reduction of $E/\mathbb{Q}$ modulo p for some prime p. We say that E has good reduction at p if $\overline{E}$ is nonsingular. We say that E has split multiplicative reduction (or semistable reduction) at p if $\overline{E}$ has a node and the minimal form has roots in $\mathbb{F}_p$. We say that E has non-split multiplicative reduction at p if $\overline{E}$ has a node and has minimal form with roots not in $\mathbb{F}_p$. We say that E has additive reduction (or unstable reduction) at p if $\overline{E}$ has a cusp.*

Example 6. $E : y^2 = x^3 + 35x + 5$ has good reduction at $p = 7$ because $y^2 \equiv x^3 + 5 \mod 7$ is nonsingular over $\mathbb{F}_7$. The curve $E : y^2 = x^3 - x^2 + 35$ has bad multiplicative reduction at $p = 5$ and $p = 7$. At $p = 5$ we have

$$((y-0) - 2(x-0)) \cdot ((y-0) + 2(x-0)) - x^3$$

with slopes $2, -2$. However in the case where $p = 7$, we cannot do this as -1 is not a quadratic residue in $\mathbb{F}_7$. That is,

$$y^2 + x^2 - x^3 \mod 7$$

and $y^2 + x^2$ can only be factored in $\mathbb{F}_7(i)$ but not in $\mathbb{F}_7$. The curve $E : y^2 + y = x^3 - x^2 - 10x - 20$ has additive reduction $\mod 11$ as the point $(5, 5)$ is singular (and the only one). ▷

Definition (L-function)**.** *For a prime p of good reduction for $E/\mathbb{Q}$, define N_p as the number of points of the curve modulo p. Let $a_p = p + 1 - N_p$. Define the local part at p of the L-series to be*

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2, & \text{if } E \text{ has good reduction at } p. \\ 1 - T, & \text{if } E \text{ has split multiplicative reduction at } p. \\ 1 + T, & \text{if } E \text{ has non-split multiplicative reduction at } p. \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Then the L-function of the elliptic curve E is defined to be

$$L(E, s) = \prod_{p \geq 2} \frac{1}{L_p(p^{-s})}$$

$L(E, s)$ is sometimes called the Hasse-Weil L-function of $E/\mathbb{Q}$.

Note the product defining $L(E, s)$ converges and gives an analytic function for $\Re(s) > 3/2$. This follows from Hasse's bound which implies $|a_p| \leq 2\sqrt{p}$. It is conjectured that $L(E, s)$ has an analytic continuation to the whole complex plane.

Moreover, L-functions were problematic at first because they did not converge on the entire complex plane. It was shown by Wiles (1995), Taylor and Wiles (1995) and Brueil (2001) that $L(e, s)$ continues to the whole complex plane and satisfied the function equation (below).

Proposition. *Let $E/\mathbb{Q}$ be an elliptic curve and let $L(E, s)$ be its L-function. Define Fourier coefficients a_n for $n \geq 1$ as follows: let $a_1 = 1$. If $p \geq 2$ is prime, define*

$$a_p = \begin{cases} p + 1 - N_p, & \text{if } E \text{ has good reduction at } p. \\ 1, & \text{if } E \text{ has split multiplicative reduction at } p. \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } p. \\ 0, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

If $n = p^r$ for some $r \geq 1$, define a_{p^r} recursively using

$$a_p \cdot a_{p^r} = a_{p^{r+1}} + p \cdot a_{p^{r-1}}, \qquad \text{if } E/\mathbb{Q} \text{ has good reduction at } p.$$

and $a_p \cdot a_{p^r}$ if $E/\mathbb{Q}$ has bad reduction at p. Finally, if $(m,n) = 1$ then define $a_{mn} = a_m \cdot a_n$. Then the L-function of E can be written as the series

$$L(E,s) = \sum_{n \geq 0} \frac{a_n}{n^s}$$

Definition (Conductor)**.** *For each prime $p \in \mathbb{Z}$, define f_p as follows:*

$$f_p = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p. \\ 1, & \text{if } E \text{ has split multiplicative reduction at } p. \\ 2, & \text{if } E \text{ has non-split multiplicative reduction at } p. \\ 2+\delta_p, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

where δ_p is a technical invariant that describes whether there is wild ramification in the action of the inertia group at p of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $T_p(E)$. Then the conductor $N_{E/\mathbb{Q}}$ of $E/\mathbb{Q}$ is defined to be

$$N_{E/\mathbb{Q}} = \prod_p p^{f_p}$$

Proposition (Conjectural Functional Equation)**.** *The L-series $L(E,s)$ has an analytic continuation to the entire complex plane, and it satisfies the following functional equation. Define*

$$\Lambda(E,s) = (N_{E/\mathbb{Q}})^{s/2}(2\pi) - s\Gamma(s)L(E,s)$$

where $N_{E/\mathbb{Q}}$ is the conductor of E and $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\,dt$ is the Gamma function. Then:

$$\Lambda(E,s) = w \cdot \Lambda(E, 2-s) \quad \text{with } w = \pm 1$$

The number $w = w(E/\mathbb{Q})$ is usually called the root number of E.

This is now a Theorem due to the Taniyama-Shimura-Weil conjecture proved by Wiles, Taylor-Wiles, Brueil, Conrad, Diamond, and Taylor.

The *analytic rank* of E is ρ, the order of zero of $L(E,s)$ at $s = 1$. The weak form of the Birch and Swinnerton-Dyer conjecture says that the analytic rank, ρ, is the same as the algebraic rank, r. The strong form gives this leading coefficient, C_0 (found below).

Proposition (Birch and Swinnerton-Dyer)**.** *Assume that $L(E,s)$ has an analytic continuation to C and satisfies the functional equation described above. Then:*

1. *$L(E,s)$ has a zero at $s = 1$ of order equal to the rank R_E of $E(\mathbb{Q})$. In other words, the Taylor expansion of $L(E,s)$ at $s = 1$ is of the form:*

$$L(E,s) = C_0 \cdot (s-1)^{R_E} + C_1 \cdot (s-1)^{R_E+1} + C_3 \cdot (s-1)^{R_E+2} + \cdots$$

   where C_0 is a non-zero constant.

2. *The residue of $L(E,s)$ at $s = 1$, i.e. the coefficient C_0, has a concrete expression in terms of invariants of $E/\mathbb{Q}$. More concretely*

$$C_0 = \lim_{s \to 1} \frac{L(E,s)}{(s-1)^{R_E}} = \frac{|Ш| \cdot \Omega_E \cdot Reg(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{torsion}(\mathbb{Q})|^2}$$

Where

1. *R_E is the (free) rank of $E(\mathbb{Q})$.*
2. *$\Omega_E = \int_{E(\mathbb{R})} \left|\frac{dx}{y}\right|$ is either the real period or twice the real period of a minimal model for E, depending on whether $E(\mathbb{R})$ is connected or not.*
3. *Ш is the order of the Shafarevich-Tate group of $E/\mathbb{Q}$.*
4. *$Reg(E/\mathbb{Q})$ is the elliptic regular of $E(\mathbb{Q})$*
5. *$|E(\mathbb{Q})_{torsion}$ is the number of torsion points on $E/\mathbb{Q}$, including $\mathcal{O}$.*
6. *c_p is an elementary local factor, equal to the cardinality of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points in $E(\mathbb{Q}_p)$ whose reduction modulo p is non-singular in $E(\mathbb{F}_p)$. Notice that if p is a prime of good reduction for $E/\mathbb{Q}$ then $c_p = 1$, so only $c_p \neq 1$ only for finitely many primes p. The number c_p is usually called the Tamagawa number of E at p.*

John Tate said of BSD: "This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined ($s = 1$) to the order of a group (Ш) which is not known to be finite!"

$E/\mathbb{Q} : y^2 = x^3 - 1156x$	
R_E	$2, \langle P = (-16, 120), Q = (-2, 48)\rangle$
$\|Ш\|$	1
Ω_E	$0.8993583214\ldots$
$\mathrm{Reg}(E/\mathbb{Q})$	$\det \mathcal{H}(\{P, Q\}) = 7.0996751824\ldots$
$E(\mathbb{Q})_{\mathrm{torsion}}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle (0,0), (34,0)\rangle$
$\prod_{p>2} c_p$	$c_2 \cdot c_{17} = 4 \cdot 4$

Figure 3: An example calculation of BSD for $E/\mathbb{Q} : y^2 = x^3 - 1156x$. We have $\frac{|Ш| \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\mathrm{torsion}}(\mathbb{Q})|^2} = 6.3851519548$.

Much is known about when the field is a number field but not as much in the "minimal" example of $\mathbb{Q}$. But much of the evidence lies in the way of calculations and not theorems. However, the evidence pointing towards its validity grows all the time and is generally believed to be true. One of the strongest pieces of evidence is:

Theorem (Gross-Zagier, Kolyvagin)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of algebraic rank R_E. Suppose that the analytic rank of $E/\mathbb{Q}$ is ≤ 1; that is, $ord_{s=1}L(E, s) \leq 1$. Then:*

1. *The first part of BSD holds for $E/\mathbb{Q}$. That is,*

$$R_e = rank(E(\mathbb{Q})) = rank_{an}(E/\mathbb{Q}) = ord_{s=1}L(E, s)$$

2. *The Shafarevich-Tate group Ш associated to $E/\mathbb{Q}$ is finite.*

It is also known that if the analytic rank, ρ, is 0 or 1 then the BSD holds for the elliptic curve E.

But of course, solving this problem (or giving a counterexample) earns one the "easiest" way of earning $1,000,000 - the price offered by the Clay Foundation for such a proof (or counterexample).