Birch and Swinnerton Dyer Conjecture

Jacobs University Bremen

2021

The millenium problems

Seven Problems in mathematics put forth by the Clay mathematics institute on May 24 2000 with a million dollar bounty on each of them.

- P versus NP
- Hodge Conjecture
- Riemann Hypothesis
- Yand-Mills existence and mass gap
- Navier-Stokes existence and smoothness
- Birch and Swinnerton-Dyer conjecture

Polynomials, Conics

There is a great interest in the problem of finding the rational solutions from polynomials. The case of single variable polynomials:

$$a_1 x^n + a_2 x^{n-1} + a_3 x^{n-2} + \cdots + a_{n+1}$$

The rational solutions can be determined using the rational root theorem. The method of finding the rational roots to the equation:

$$X^2 + y^2 = \mathbb{R}$$

is quite well defined as well. (Hasse-Minkowski)

Rational Solutions in Conics

Let $f(x, y)$ be a quadratic polynomial in x and y with rational coefficients. Then the set of all rational points (x, y) on the conic $f(x, y) = 0$ is either:

- Empty;
- in one-to-one correspondence with slopes in $\mathbb{Q} \cup \infty$.

In the second case, one can explicitly find all rational points as follows:

- Start with a base rational point P on the conic;
- Take all lines of rational slope through P;
- Compute the second point of intersection of each of these lines with the conic $f(x, y) = 0$.

Cubics

We run into problems when we go to a two variable equation of degree 3.

$$Y^3 + X^3 = \mathbb{R}$$

There are three possible cases with such equations:

- No rational solutions
- Finite rational solution
- Infinite rational solutions

However, finding which case the equation is in, is itself an unsolved problem. I.e. we have no reliable self terminating algorithm that gives which case a given cubic equation is in.

Elliptic curve

Given a smooth cubic equation, $f(x, y) = 0$ that has rational solution $P(x_0, y_0)$ one can effect a rational change of variable such that P is sent to infinity in such a way, the equation of the cubic becomes:

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

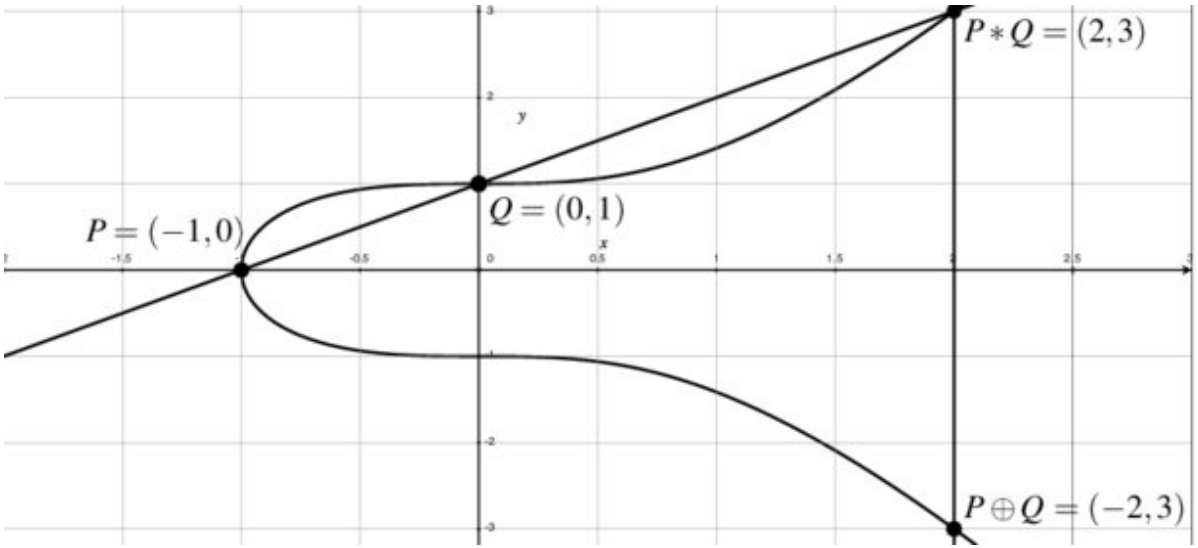
where A and B are integers and $\Delta = -4A^3 - 27B^2 \neq 0$ (Silverman-Tate)

An equation of this type is called an elliptic curve in Weierstrass form.

Group law on elliptic curves

Given two rational points P and Q on a plane elliptic curve E, the line connecting P and Q intersects with E at another rational point.

We may define the rational point $P + Q$ on E as:



Together with the point at infinity as the identity, this law of addition imposes the structure of an abelian group into the set of rational points on E

Mordell's Theorem

For a rational elliptic curve E, the group on rational points on E is denoted by $E(\mathbb{Q})$.

Mordell's Theorem: *The group $E(\mathbb{Q})$ of rational points on E is finitely generated.*

Because $E(\mathbb{Q}$ is finitely generated, the fundamental theorem of abelian groups says that:

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

for some $r \geq 0$ and T a finite abelian group.
It is a theorem of Mazur that the group T is bounded in size by 16. Thus, r measures how big $E(\mathbb{Q})$ actually is. r is called the rank of E. It gives the number of points needed to generate all rational points on the curve, and as a consequence of Mordell's theorem, this number is always finite.

How do we proceed now?

Given these properties for elliptic curves, one may ask the following questions to help them find its rational points:

- Is there a maximum to the rank of an elliptic curve? If yes, what is it?
- What is the expected size of the rank?
- Do most curves have rank 0 or 1?
- Is there any algorithm to determine the rank of an elliptic curve, which will terminate and with the correct answer?

The Birch and Swinnerton-Dyer conjecture addresses the last question.

Solution mod p

In a lot of cases, it is too computationally expensive to look at solutions over the entire set of real numbers. To optimise for this constraint, it is often useful to just look at a smaller subset of the space. Instead of looking at solutions, we look at solutions *mod* p (where p is a prime number) over the curve *mod* p

The Birch and Swinnerton-Dyer Conjecture

In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves, and of the number of solutions mod p on these elliptic curves.

In general, if $E : y^2 = x^3 + Ax + B$ is a random elliptic curve, then one expects that modulo p it should have about p points. Thus one expects that N_p/p should be about 1 most of the time.

However, if E has lots of rational points on it, then these points mod p would give lots of points on the elliptic curve $(\mathrm{mod}\, p)$. Birch and Swinnerton-Dyer hypothesized that if the rank of the elliptic curve E is large, then on average one should notice E having more than p points modulo p in that case.

The Birch and Swinnerton Dyer Conjecture

Conjecture (Birch and Swinnerton-Dyer). Let E be an elliptic curve, let r be its rank, and let N_p denote the number of points on $E(\mathrm{mod}\, p)$. Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

(Birch and Swinnerton-Dyer also gave an explicit expression for c in terms of E; this is called the strong form of the conjecture.)

Modern Formulation

Let E be an elliptic curve, and let N_p denote the number of points on $E(\mathrm{mod}\, p)$.
Set $a_p = p + 1 - N_p$, and define the incomplete L -function of E by

$$L(E, s) = \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Although this product converges only for $s \in \mathbb{C}$ satisfying $\mathrm{Re}(s) > 3/2$, a conjecture of Hasse states that $L(E, s)$ should have a analytic continuation as a function of s to the entire complex plane! It then makes sense to speak of the value and order of vanishing of this analytic function of s at $s = 1$. (The partial products of this function at $s = 1$ are exactly the reciprocals of the expressions $\prod_{p \leq X} N_p/p$.)

How The Modern Formulation Makes Sense ?

Theorem (Wiles et al 1995). For any E, the L-function $L(E, s)$ has a analytic continuation to the entire complex plane.

Let E be an elliptic curve, and let r be its rank. By the above theorem of Wiles et al, there exists an integer r' such that the Taylor expansion of $L(E, s)$ at $s = 1$ is of the form

$$a(s-1)^{r'} + \text{ higher order terms}$$

with $a \neq 0$. The quantity r' is called the analytic rank of E.

Conjecture (Birch and Swinnerton-Dyer). The rank of E is equal to the analytic rank of E, i.e., $r = r'$.

What is Known about the BSD ?

Theorem (Coates and Wiles 1977). If E is an elliptic curve of the form $y^2 = x^3 + Ax$ or $y^2 = x^3 + B$, and if $r' = 0$, then the *BSD* Conjecture is true for E.

Theorem (Gross, Zagier, and Kolyvagin 1989). If $r' = 0$ or 1 for an elliptic curve E, then the BSD Conjecture is true for E.

Theorem (Skinner, Urban, and Zhang 2013). If $r = 0$ or 1 for an elliptic curve E, and if E satisfies some further technical conditions.

Height of an Elliptic Curve

Recall that we may write any elliptic curve E over the rational numbers in the form

$$E_{A,B} : y^2 = x^3 + Ax + B$$

where A and B are integers. We may then define the height of E by the size of the coefficients of the defining equation.
If $E = E_{A,B}$, then $H(E_{A,B}) := \max\left\{4|A|^3, 27B^2\right\}$. This is called the (naive) height of E.
We can then list all elliptic curves $E/\mathbb{Q}$ in order of increasing height, and ask statistical questions relating to the rank and to the probability that BSD is satisfied for these elliptic curves.

What is Known about the BSD ?

We now know that most elliptic curves have rank 0 or 1 : **Theorem (Manjul Bhargava and Arul Shankar 2013):** At least 83% of all elliptic curves have rank O or 1.

In fact, the methods in particular establish some of the technical conditions that Skinner, Urban, and Zhang require to deduce that: Corollary of Proof: A positive proportion of elliptic curves satisfy *BSD*.

What proportion do all current results actually allow us to prove? **Theorem (Manjul Bhargava,Christopher Skinner and Wei Zhang)**. The Birch and Swinnerton-Dyer Conjecture is true for more than 66% of all elliptic curves.

What Remains To be done?

- Everything we have talked about so far has been about curves of Rank 0 or 1, which are conjectured to be 100% of elliptic curves.
- The technical conditions in the theorem of Skinner, Urban, and Zhang must still be removed; once this is accomplished, this would likely mean that we understand BSD for 100% of elliptic curves!
- However, it is the remaining 0% of curves, having rank at least 2 , that has been causing mathematicians the greatest difficulty!
- Q While rare, there are infinitely many elliptic curves having rank at least 2, and for such curves essentially nothing is known regarding BSD. This is where the next big idea is needed!
- There are now many beautiful extensions of the BSD Conjecture and the above-mentioned results about it including the BlochKato Conjecture,