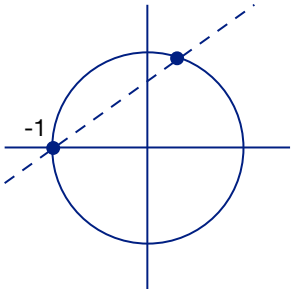
Manjul Bhargava

Manjul Bhargava spoke about elliptic curves and the Birch and Swinnerton-Dyer Conjecture (BSD), one of the most fundamental probelms in number theory. He explained its origin and its statement in elementary terms, as well as summarising progress towards a proof, including results that were emerging in the workshop taking place during week of the Research Conference.

A central theme of number theory is the search for rational solutions of polynomial equations. For a polynomial in one variable with integer coefficients, the problem is easily solved by using the Rational Root Theorem. Two variable equations are more interesting.

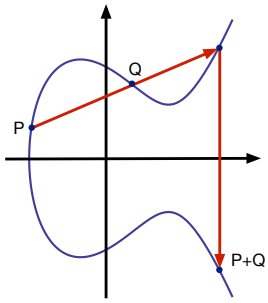


Equations of degree one in two variables are easy. The degree two case is not much more difficult. A simple geometric argument, for example, puts the rational points on the circle $x^2 + y^2 = 1$ (the points with rational coordinates) into correspondence with $\mathbb{Q} \cup \{\infty\}$, by noting that the rational points are the intersections with the circle of lines through $(-1, 0)$ with slope $s \in \mathbb{Q}$. The point $(-1, 0)$ itself is labelled by $s = \infty$.

The Hasse-Minkowski theorem gives an algorithm for determining whether or not a general conic contains any rational points. Provided that there is at least one rational point, the same procedure as for the circle works for a general conic, with the rational point replacing $(-1, 0)$

For two-variable equations of degree three, the probelm is much more difficult. A given equation may have no rational solutions, a positive finite number of solutions, or infinitiely many solutions, but it is already an unsolved problem to determine which. This is where the BSD conjecture comes in: if true, it would provide a method to determine all the rational solutions, and in particular to determine whether there are finitely or infinitely many such solutions. So BSD is the key to understanding degree three equations.

What then is the Birch and Swinnerton-Dyer conjecture? Uniquely in the cubic case, the set of rational points on a cubic curve has the structure of an abelian group (the *divisor class group*). Assume that we are given a smooth cubic equation $f(x, y) = 0$ (i.e. the curve is smooth) with at least one rational solution $P = (x_0, y_0)$. By a rational change of variables, P can be sent to infinity and the equation reduced to



$$y^2 = x^3 + Ax + B \quad (*)$$

where, for smoothness, the discriminant $\Delta = -4A^3 - 27B^2$ is nonzero. We then have an *elliptic curve* $E = E_{A,B}$ *in Weierstrass form*.

Given two rational points P, Q on E, the line through them intersects E in a third point. The group law is defined by taking the sum $P + Q$ to be the third point, reflected in the x-axis. The identity is the point at infinity.

A lot is known about the group $E(\mathbb{Q})$ of rational points on E. To begin with, we have Mordell's theorem that $E(\mathbb{Q})$ is finitely generated. Since it is also abelian, it must be of the form

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

for some $r \geq 0$ and some finite abelian group T. A theorem of Mazur's establishes that $|T|$ cannot exceed 16.

The invariant r is called the *rank* of E. It measures the size of $E(\mathbb{Q})$. In particular if $r = 0$ then E has only finitely many rational points while if $r > 0$, there are infinitely many.

A lot of questions about ranks of elliptic curves are unsolved: it is not known if there is an upper bound (in the most extreme known example, found by Elkies, the rank is at least 28); very little is known about the distribution of r as A, B vary; most mathematicians believe that 100% of elliptic curves have rank 0 or 1 in an appropriate probabilistic sense—this has not been proved, although it has been shown recently that at least 1% do; it is not known whether or not there is an algorithm to determine the rank that provably terminates with the correct answer. The BSD conjecture addresses this last question.

The formulation of the BSD conjecture begins with consideration of the number of solutions to $(*)$ mod p, a prime. An arbitrary choice for x mod p will give a solution mod p if the $x^3 + Ax + B$ is a square mod p. This will happen in general for about half the choices made for x, and each time it does happen there are two possible values of y. So there should be about p solutions mod p.

If E contains many rational points then by reducing their coordinates mod p, one obtains lots of solutions to $(*)$ (mod p). Birch and Swinnerton-Dyer hypothesized that if the rank of E is large then on average E should have more than p points (mod p). After many computations to check this, they arrived at

> **Conjecture (Birch and Swinnerton-Dyer)**. Let E be an elliptic curve over $\mathbb{Q}$, let r be its rank, and let N_p denote the number of points on E (mod p). Then
>
> $$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r \qquad (**)$$
>
> for some constant c.

The strong form of the conjecture includes an expression for c in terms of arithmetic invariants of E.

A modern form of the conjecture involves the behavior of the *incomplete L-function* of E, which is defined by

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

where $a_p = p + 1 - N_p$. The partial products at $s = 1$ are precisely the expressions on the left-hand side of $(**)$. A heuristic argument suggests that if the rank of E is large then p/N_p should be small and the product should vanish. Although the product itself only converges for $\mathrm{Re}(s) > 3/2$ one can still make sense of this: it was conjectured by Hasse and proved by Wiles and others that L extends to an entire function of s, as a consequence of the modularity theorem. In terms of L, the BSD conjecture is that $r = r'$, where r' is the order of the zero of L at $s = 1$ (in fact this is weaker than Birch and Swinnerton-Dyer's original formulation).

The interger r' is called the *analytic rank* of E. The conjecture is remarkable in equating r', which is defined analytically, to r (sometimes called the 'algebraic rank'), which is defined algebraically.

What is known about BSD?

- In 1977, Coates and Wiles showed that BSD is true when E is of the form $y^2 = x^3 + Ax$ or $y^2 = x^3 + B$, and $r' = 0$.
- In 1989, Gross, Zagier, and Kolyvagin showed that BSD is true when $r' = 0$ or $r' = 1$.
- In 2013, Skinner, Urban, and Zhang showed that if $r = 0$ or $r = 1$ and if E satisfies some further conditions, then BSD is true; the list of further conditions has since been reduced, not least during the 2016 Clay workshop.

Do any elliptic curves satisfy these conditions? Define the *height* of $E = E_{A,B}$ to be $\max\{4|A|^3, 27B^2\}$ and list elliptic curves $E/\mathbb{Q}$ in order of increasing height. One can then ask statistical questions about the probability that BSD holds.

- In 2013, Bhargava and Shankar showed that at least 83% of elliptic curves have $r = 0$ or $r = 1$.

Because a proportion of the 83% satisfy the further conditions, it follows that *a positive proportion of elliptic curves satisfy BSD*. In fact Bhargava, Skinner, and Wei Zhang have shown that BSD is true for 66% of all elliptic curves. This percentage has risen during the workshop.

A lot remains to be done. The 'further conditions' are still to be eliminated to establish BSD for elliptic curves of rank zero or one. These are conjectured to be 100% of all curves in a probability sense. But there remain infinitely many elliptic

curves of higher rank. For them, essentially nothing is known. There are also many beautiful generalizations of the conjecture: extensions to higher dimensions, to p-adic analogues, and to curves over number fields.