The Birch and Swinnerton-Dyer conjecture

Proposal Text

Amod Agashe

1 Project description

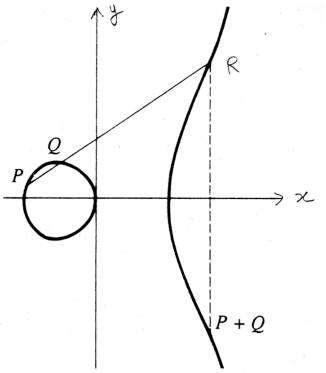
This project lies in the area of number theory, and in particular in a subarea called arithmetic geometry. Our main objects of interest are elliptic curves, which we define in Section 1.1 below. The main question regarding elliptic curves that we plan to tackle is the Birch and Swinnerton-Dyer conjecture, which we discuss in Section 1.2. Finally we describe what we plan to accomplish regarding this conjecture in Section 1.3.

1.1 Elliptic curves

For centuries, mathematicians have been interested in finding integer or rational solutions to polynomial equations. For example, consider the equation $x^2 + y^2 = z^2$, whose solutions (x, y, z) correspond to the sides of right-angled triangles, and hence are called *Pythagorean triples*. An example of a solution to this equation is the familiar triple $x = 3$, $y = 4$, and $z = 5$. In fact, there are infinitely many rational solutions to this equation: take any integer t; then $x = 2t$, $y = t^2 - 1$, and $z = t^2 - 1$ gives a solution. Polynomial equations whose coefficients are integers or rational numbers are called *Diophantine equations*, and the study of their integer or rational solutions is called *arithmetic geometry*. In the example of the equation $x^2 + y^2 = z^2$ above, the parametrization $x = 2t$, $y = t^2 - 1$, and $z = t^2 - 1$, where t ranges over all integers, describes all the solutions. Some equations may not have any rational solutions, e.g., $x^2 + y^2 = -1$ does not have a solution since the sum of the squares of two rational numbers cannot be negative.

The problem of describing all the solutions to a general polynomial equation is too complicated, and perhaps does not have a nice answer in any case. So we focus on the slightly simpler problem of problem of deciding if there are finitely many or infinitely many solutions to a given equation. For example, by the discussion above, the equation $x^2 + y^2 = z^2$ has infinitely many solutions, while the equation $x^2 + y^2 = -1$ has finitely many (in fact, zero) solutions. For most equations, the problem of deciding whether the number of solutions is finite or infinite is well resolved, with one exception: the class of elliptic curves, which we now define.

An *elliptic curve* is the set of solutions to an equation of the form $y^2 = x^3 + ax + b$, where a and b are rational numbers such that $4a^3 + 27b^2 \neq 0$. For example, if we take $a = -1$ and $b = 0$, then we get the equation $y^2 = x^3 - x$, whose graph consists of the two thick curved pieces in the figure below:



What we have sketched in the figure above is the set of all pairs (x, y) such that x and y are real numbers that satisfy $y^2 = x^3 - x$. Our interest is in the set of points on the curve above whose coordinates are in fact rational numbers; such points will be called *rational points* on the elliptic curve or *rational solutions* to the equation defining the elliptic curve. For example, $(1, 0)$ is a rational point on the curve $y^2 = x^3 - x$ sketched in the figure above; the point $(2, \sqrt{6})$ can also be seen to lie on the curve, but it is not rational. One of the important open problems that we plan to tackle is the following: decide if a the equation of a given elliptic curve has finitely many or infinitely many rational solutions. For a randomly chosen elliptic curve, this problem is so difficult that the only known approach (the Birch and Swinnerton-Dyer conjecture) carries a million dollar reward for its resolution.

One of the nice properties of elliptic curves is that given two points P and Q on the curve, we can find a third point, called the "sum" of P and Q, and denoted $P + Q$, as follows. We first join P and Q by a straight line. This straight line will intersect the curve at a third point; call it R. Then we draw a vertical line through R, which will interesect the curve at another point; we define $P + Q$ to be this latter point. This process is illustrated in the figure above. If P and Q are rational points, then so is $P + Q$. We remark that the procedure above works for almost all pairs of points: there are some exceptional cases where one has to be more careful, but we omit the details for simplicity. In fact, for the interested reader, at the website `http://www.certicom.com/index.php?action=ecc,ecc_tut_2_3` there is a java applet using which one can easily sketch elliptic curves corresponding to different equations, select two points on the curve, and find the sum of the points.

Any set on which we can define a sum of two elements in a way that the usual laws of addition are obeyed is called a *group*. The simplest example of a group is the set of integers with the usual addition operation; this group is denoted $\mathbf{Z}$. As another example, pick a non-zero integer m, and consider the set of integers from 0 to $m - 1$. Given two integers a and b in this set, define their sum, denoted $a \oplus b$, as the remainder obtained when one divides $a + b$ by m. The resulting group is denoted $\mathbf{Z}/m\mathbf{Z}$ and is called the group of integers modulo m. For example, if we take $m = 2$, then the group consists of two elements: 0 and 1, and the addition law is given by $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, and $1 \oplus 1 = 1$.

Finally, from the discussion above, the set of rational solutions to an equation defining an elliptic curve from a group. While so far we have been looking for rational solutions to the elliptic curve, we take a slight detour to discuss other possible solutions, which play an important role in cryptography and are also relevant to the project description. If the curve is given by $y^2 = x^3 + ax + b$ and a and b are integers, then one can look for solutions x and y that are in the set of integers modulo p for a prime number p. It turns out that one can define an addition law on this new set of solutions as we did before; this set is necessarily finite, and thus gives a group that is finite in size. For example, we can consider the solutions modulo 2 to the curve $y^2 = x^3 - x$: the only solutions are $(x, y) = (0, 0)$ and $(1, 0)$: $(0, 1)$ and $(1, 1)$ do not satisfy the equation.

Such finite groups coming from elliptic curves find several applications in cryptography, and elliptic curve based cryptosystems are competing well with the traditional RSA based cryptosystems. While the PI does not plan to directly work on the applications of elliptic curves to cryptography as a part of this research proposal, he has worked on such applications to cryptography in the past, and is quite likely to do so in the future. In fact, he is advising a doctoral student in the area of cryptography. In any case, we want to emphasize that apart from being objects of intrinsic mathematical interest, elliptic curves are interesting from the real-world point of view as well.

1.2 Birch and Swinnerton-Dyer conjecture

Let us get back to our primary object of interest: the set of rational solutions to an equation defining an elliptic curve. Recall that this set is in fact a group. This group can be broken into two into disjoint pieces that are themselves groups:
1) An infinite part, which can be broken into a finite number of disjoint copies of the group of integers $\mathbf{Z}$, and
2) A finite part, which can be broken into a finite number of disjoint copies of the group $\mathbf{Z}/m\mathbf{Z}$ of integers modulo m, for certain integers m.

Thus the problem of describing the rational solutions to an elliptic curve boils down to the following question: how many copies of $\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$ (for various m's) occur in the decomposition above? In particular, the number of rational solutions is finite if and only if there is no copy of $\mathbf{Z}$ in the decomposition.

It turns out that for a given elliptic curve, it is not too difficult to compute the number of copies of $\mathbf{Z}/m\mathbf{Z}$ (for various m's) that occur in the decomposition above, and the question reduces to that of finding the number of copies of $\mathbf{Z}$ that appear in the decomposition. The Birch and Swinnerton-Dyer conjecture (henceforth abbreviated BSD conjecture) gives a conjectural answer to this latter problem. In order to state the conjecture, we need to define the L-function of an elliptic curve E. If p is a prime number, then let $N_p(E)$ denote the number of solutions to the equation defining E in the set of integers modulo p. For example, in the example of the elliptic curve $y^2 = x^3 - x$ discussed at the end of the previous section, $N_2(E) = 2$ (since the only solutions were $(0,0)$ and $(1,1)$). For an elliptic curve E, we define its L-function as follows:

$$L_E(s) = \prod_{p \nmid 2(4a^3+27b^2)} (1 + (N_p(E) - p)p^{-s} + p^{1-2s})^{-1}.$$

In reality, one has to use a modified definition to overcome certain technical problems, but we will skip the details for the sake of simplicity. One should think of the L-function as being obtained by packaging information about the number of solutions to E in the set of integers modulo p for all primes p.

The first part of the BSD conjecture says that the number of copies of $\mathbf{Z}$ in the group of rational solutions to E is the order of vanishing of $L_E(s)$ at $s = 1$. In particular, it says that the number of rational solutions is infinite if and only if $L_E(1) = 0$. It turns out that for a given elliptic curve E, it is rather easy to decide if $L_E(1)$ is zero or non-zero, and thus if the conjecture were to be proved true, then it would provide us with a practical algorithm for deciding if the number of rational solutions to an equation of the form $y^2 = x^3 + ax + b = 0$ is finite or infinite. Recall that these were the only curves for which the issue of finiteness of solutions was unresolved. Thus a proof the BSD conjecture would fill in an important missing chapter in the theory of Diophantine equations.

There is a second part to the BSD conjecture, which gives a fomula for the leading term in the Taylor series expansion of $L_E(s)$ at $s = 1$ in terms of the sizes of certain groups associated to E. In particular, one of the groups involved is the finite part of the group of rational points on the elliptic curve.

1.3 The project

The PI plans to work on both the first and second parts of the BSD conjecture. The first part of the conjecture has been proved by Kolyvagin and Gross-Zagier in the cases where the order of vanishing of $L_E(s)$ at $s = 1$ is either 0 or 1. One of the projects that the PI plans to undertake is

to extend the ideas behind the result of Gross-Zagier to the situation where the order of vanishing is greater than 1. This is a difficult and long-term project.

Regarding the second part of the BSD conjecture, the PI has been working on it for the past five years and has several publications on it already. The PI has been focussing on the case where $L_E(1) \neq 0$ and trying to show that the left hand side of the conjectured formula divides the right hand side; this should suffice to prove the formula since luckily the divisibility in the other direction is already known in several cases. So far the PI has been able to relate a certain piece of the left side of the conjectural equality to the right hand side. There is another piece on the left side that is a mystery, and the PI plans to look at it more closely in this proposal. We already have some ideas on this problem, which we will try out.

As mentioned above, the second part of the BSD conjecture also involves the finite part of the group of rational points on an elliptic curve. The PI plans to characterize the order of this finite part for a general elliptic curve E. This, together with a solution of the first part of the BSD conjecture, would give a complete answer to the question of describing all the solutions to the equation defining an elliptic curve.

2 Previous activities

a) Dissertation Title: The Birch and Swinnerton-Dyer formula for modular abelian varieties.

In this work, the PI gave a formula for the quantity $L_E(1)$ that appears in the second part of the Birch and Swinnerton-Dyer (BSD) conjecture. Most of the PI's current proposal is about the certain other parts of the BSD conjecture, which is a much bigger problem. Thus the current proposal is a substantive departure from the PI's dissertation.

3 Significance of the project

The Birch and Swinnerton-Dyer (BSD) conjecture is clearly one of the important problems in mathematics: it describes the set of rational solutions to equations defining an elliptic curve. As we mentioned in Section 1.1, there are the only curves for which no algorithm is known to decide whether the number of rational solutions is finite or infinite; a proof of the BSD conjecture would resolve this remaining issue. The importance of the conjecture can be judged by the fact that it was selected as one of the seven millenial prize problems by the Clay mathematics institute, and carries a million dollor reward for its resolution.

Apart from intrinsic mathematical interest, work on the BSD conjecture also helps us understand elliptic curves, which, as mentioned before, have found practical applications to cryptography. There are already some potential application of the BSD conjecture to cryptography, which are waiting for the conjecture to be proved.

4 Keywords

Number theory, Arithmetic geometry, Diophantine equations, Elliptic curve, L-function, Birch and Swinnerton-Dyer conjecture, group, Shafarevich-Tate group.