Elliptic curves, modularity and the conjecture of Birch and Swinnerton-Dyer

Peter Bruin

17 May 2016

Contents

1 Introduction

As mentioned in the previous lecture, there exists an important connection between modular forms and elliptic curves by means of their L-functions. Since knowledge of elliptic curves is not a prerequisite for this course, in this lecture we will introduce some background on elliptic curves that will enable us to explain this connection. Two illustrations of the connection between L-functions and modular forms are the modularity theorem for elliptic curves over $\mathbf{Q}$ and the conjecture of Birch and Swinnerton-Dyer.

The modularity theorem predicts that the L-function attached to any elliptic curve over $\mathbf{Q}$ is also the L-function of some primitive cusp form. This was stated as a conjecture by Shimura and Taniyama in the 1950s. Around 1995, Andrew Wiles (with the help of Richard Taylor) proved enough of the modularity theorem to deduce Fermat's last theorem. The proof of the modularity theorem was completed in 2001 by the work of Breuil, Conrad, Diamond and Taylor.

An elliptic curve E over $\mathbf{Q}$ has an L-function $L(E, s)$, which is defined purely in terms of *local* data (the reductions of E modulo prime numbers). The conjecture of Birch and Swinnerton-Dyer predicts the behaviour of the function $L(E, s)$ at the point $s = 1$ in terms of *global* data (the rank of the group of rational points). This conjecture can be compared to the analytic class number formula from algebraic number theory, which links the residue at $s = 1$ of the Dedekind ζ-function $\zeta_K(s)$ of a number field K to various arithmetic invariants attached to K.

2 Elliptic curves

We first give a 'canonical' definition of elliptic curves, and then say somewhat more concretely what an equation for an elliptic curve looks like.

Definition. An *elliptic curve* over a field K is a smooth cubic curve E in the projective plane over K together with a K-rational point $O \in E(K)$.

After a suitable choice of coordinates, every elliptic curve over K is given by a *Weierstrass equation*. This is a homogeneous equation of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $a_1, \ldots, a_6 \in K$ (subject to some condition expressing the smoothness of E), with the point O having coordinates $(0 : 1 : 0)$. This is usually written in affine coordinates as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We write $E(K)$ for the set of all K-rational points of E. This can be thought of as the set of all pairs $(x, y) \in K \times K$ satisfying the above equation, together with the 'infinite' point O.

One of the most fundamental facts about elliptic curves is that the set $E(K)$ has the structure of an Abelian group with identity element O. The group structure is determined uniquely by the property that three points add up to O if and only if they are the three intersection points (counted with multiplicities) of E with a line.

For elliptic curves over $\mathbf{Q}$ (or more general number fields), the structure of $E(K)$ has been studied very extensively. The basic result about $E(K)$ in this case is the *Mordell–Weil theorem*.

Theorem 2.1 (Mordell–Weil)**.** *If $K = \mathbf{Q}$ (or more generally any number field), then the Abelian group $E(K)$ is finitely generated.*

If E is an elliptic curve over a number field K, then $E(K)$ is called the *Mordell–Weil group* of E. The above theorem implies that if E is an elliptic curve over $\mathbf{Q}$, we can write

$$E(\mathbf{Q}) = T \times \mathbf{Z}^r,$$

where T is a finite Abelian group (the torsion subgroup $E(\mathbf{Q})_{\mathrm{tor}}$ of $E(\mathbf{Q})$) and r is some non-negative integer, called the *(algebraic) rank* of E.

Given an elliptic curve E over $\mathbf{Q}$, there is a straightforward way of computing $E(\mathbf{Q})_{\mathrm{tor}}$, and there are only finitely many possibilities for the group $E(\mathbf{Q})_{\mathrm{tor}}$ up to isomorphism. However, it is in general much harder to determine r, and it is not known whether r can be arbitrarily large. Furthermore, it is in general 'hard' to determine a finite set of points $P_1, \ldots, P_r \in E(\mathbf{Q})$ such that $P_1, \ldots, P_r$ together with $E(\mathbf{Q})_{\mathrm{tor}}$ is a generating set of $E(\mathbf{Q})$.

3 The L-function of an elliptic curve

We assume that E is an elliptic curve over $\mathbf{Q}$ given by a Weierstrass equation as above, and such that in addition the a_i are in $\mathbf{Z}$ and the equation is *minimal* (a notion that we will not make precise). Then for every prime number p, we consider the equation over $\mathbf{F}_p$ obtained by reducing the equation modulo p. The curve $E_{\mathbf{F}_p}$ defined by this equation is called the *reduction of E modulo p*.

We say that E has *good reduction* at p if $E_{\mathbf{F}_p}$ is a smooth curve; otherwise we say that E has *bad reduction* at p. There exists a positive integer N (called the *conductor* of E, and related to the *minimal discriminant* of E) such that E has bad reduction at p if and only if $p \mid N$. In particular, E only has bad reduction at finitely many prime numbers p.

For every prime number, the set $E(\mathbf{F}_p)$ is finite. We define integers a_p for p prime by

$$a_p = p + 1 - \#E(\mathbf{F}_p).$$

Remark. This is the correct definition even when the reduction of E modulo p is singular.

Theorem 3.1 (Hasse)**.** *The integers a_p satisfy*

$$|a_p| \leq 2\sqrt{p}.$$

Furthermore, we define

$$\epsilon(p) = \begin{cases} 1 & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N. \end{cases}$$

(In other words, ϵ is the trivial Dirichlet character modulo N.)

We now define

$$L(E, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}}.$$

It follows from Hasse's theorem that this infinite product converges absolutely and uniformly for $\Re s \geq \sigma$, for any $\sigma > 3/2$. This implies that the product defines a holomorphic function on $\{s \in \mathbf{C} \mid \Re s > 3/2\}$. However, unlike in the setting of modular forms, where we have the Mellin transform at our disposal, there seems to be no easy way to prove that $L(E, s)$ has an analytic continuation and functional equation.

4 The modularity theorem

To be able to say anything really interesting about the L-function of an elliptic curve over $\mathbf{Q}$, we will need the modularity theorem. This is the following statement.

Theorem 4.1 (Modularity of elliptic curves over $\mathbf{Q}$)**.** *Let E be an elliptic curve over $\mathbf{Q}$. Then there exist $N \geq 1$ and a primitive form $f \in \mathrm{S}_2(\Gamma_0(N))$ of weight 2 such that $L(f, s)$ is equal to $L(E, s)$.*

Example. Let E be the elliptic curve defined by the equation

$$E\colon y^2 + y = x^3 - x^2.$$

Then the conductor N of E equals 11. (This is the smallest possible conductor of an elliptic curve over $\mathbf{Q}$.) There exists exactly one primitive cusp form of weight 2 for $\Gamma_0(11)$, namely

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + O(q^{10}).$$

Hence this is the primitive form attached to E by the modularity theorem.

The modularity theorem (formerly the Taniyama–Shimura conjecture) is a very deep result. One of its most important consequences is that it implies that L-functions of elliptic curves over $\mathbf{Q}$ admit an analytic continuation to all of $\mathbf{C}$ and satisfy a functional equation relating $L(E, s)$ and $L(E, 2 - s)$ (again via completed L-functions, like in the case of L-functions of modular forms). This is not at all obvious, and the modularity theorem is currently the only known way to prove the analytic continuation and functional equation for L-functions of elliptic curves. For elliptic curves over other number fields than $\mathbf{Q}$, only very partial results are known.

The modularity theorem was proved first for an important class of elliptic curves (the *semi-stable* ones, corresponding to square-free N) in 1995 by work of Wiles [4], completed by Taylor and Wiles [2], from which Fermat's last theorem follows. (More about Fermat's last theorem will be said in the last lecture of this course.) The modularity theorem was then proved in more generality by Diamond (1996), Conrad, Diamond and Taylor (1999) and finally for arbitrary E by Breuil, Conrad, Diamond and Taylor (2001).

The proof of the modularity theorem combines many different techniques, which we cannot explain here. Just to mention one key part of the proof that is related to this course: one ingredient is to show that certain Hecke algebras are isomorphic to so-called *deformation rings*. This is then used to prove a *modularity lifting theorem*, which is a statement of the type that if the coefficients a_n of $L(E, s)$ are congruent to the coefficients of a modular form modulo some prime number l, then the coefficients a_n are actually *equal* to the coefficients of a modular form.

Remark. We have phrased the modularity theorem in terms of L-functions, but there are many other formulations; see Diamond and Shurman's book for alternative versions.

5 The conjecture of Birch and Swinnerton-Dyer

Around 1958, Birch and Swinnerton-Dyer performed some of the first computer calculations in number theory. Given an elliptic curve over $\mathbf{Q}$ given by a Weierstrass equation with coefficients in $\mathbf{Z}$, they studied the way in which the number of points $\#E(\mathbf{F}_p)$ of the reduction depends on the rank of E over $\mathbf{Q}$. Based on their calculations, they stated a conjecture that can be formulated in one way as follows.

Conjecture 5.1 (Birch, Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbf{Q}$. Then the order of vanishing of function $L(E, s)$ in $s = 1$ (which is defined thanks to the modularity theorem) is equal to the rank of E.*

Remark. The order of vanishing of $L(E, s)$ in $s = 1$ is called the *analytic rank* of E; hence the Birch–Swinnerton-Dyer conjecture claims that the analytic rank of an elliptic curve is equal to its algebraic rank.

The conjecture of Birch and Swinnerton-Dyer is as yet unproved. It is in fact one of the "Millennium Prize Problems"; a proof is therefore worth one million dollars. The only general result known so far is the following.

Theorem 5.2 (Gross, Zagier; Kolyvagin)**.** *Let E be an elliptic curve over $\mathbf{Q}$. If the analytic rank of E is either 0 or 1, then it is equal to the algebraic rank of E.*

The proof of this theorem heavily relies on modular forms, modular curves, L-functions and related techniques.

In addition, Bhargava and Shankar proved in recent years that a positive proportion (in a precise sense) of all elliptic curves over $\mathbf{Q}$ have analytic rank 0, which implies that the conjecture of Birch and Swinnerton-Dyer holds for a positive proportion of all elliptic curves over $\mathbf{Q}$. (It seems, however, that they have not been awarded the corresponding fraction of the prize money.)

Remark. Let r denote the analytic rank of E. We consider the non-zero complex number

$$L^*(E, s) = \lim_{s \to 1} (s - 1)^{-r} L(E, s).$$

There is a refined variant of the conjecture of Birch and Swinnerton-Dyer, which predicts the exact value of $L^*(E, s)$ in terms of certain analytic and arithmetic invariants of E (namely *periods*, *Tamagawa numbers*, the *regulator*, the order of the torsion group $E(\mathbf{Q})_{\mathrm{tor}}$, and the order of the *Tate–Shafararevich group*).

6 The congruent number problem

In this last section, we discuss how elliptic curves, modular forms and the conjecture of Birch and Swinnerton-Dyer can be applied to a classical Diophantine problem.

A positive rational number n is called *congruent* if there exists a right-angled triangle with rational side lengths and area n. The *congruent number problem* is the question which n are congruent. This comes down to the question for which n the system of equations

$$a^2 + b^2 = c^2 \quad \text{and} \quad ab = 2n$$

has a solution in non-zero rational numbers a, b, c.

Proposition 6.1. *A positive rational number n is congruent if and only if the equation*

$$y^2 = x^3 - n^2 x \tag{1}$$

has a solution $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ with $y \neq 0$.

It suffices to study the case where n is a square-free positive integer. The equation (1) defines an elliptic curve E_n over $\mathbf{Q}$. The congruent number problem was solved by Tunnell [3] assuming the Birch–Swinnerton-Dyer conjecture for elliptic curves of the form E_n. We define integers c_n for $n \geq 1$ by the following identities of holomorphic functions $\mathbf{H} \to \mathbf{C}$ (or of power series in q):

$$\begin{aligned} h &= \eta(8z)\eta(16z) \\ &= q \prod_{m \geq 1} \big((1-q^{8m})(1-q^{16m})\big), \\ f &= h\theta(2z), \\ g &= h\theta(4z), \\ c_n &= \begin{cases} a_n(f) & \text{if } n \text{ is odd,} \\ a_{n/2}(g) & \text{if } n \text{ is even.} \end{cases} \end{aligned}$$

Here η and θ are the Dedekind η-function and the Jacobi θ-function defined in the course. (The functions f and g are in fact "modular forms of weight 3/2".)

Theorem 6.2 (Tunnell [3])**.** *Let n be a square-free positive integer. If n is congruent, then $c_n = 0$. The converse is true if the Birch–Swinnerton-Dyer conjecture holds for the elliptic curve E_n.*

Tunnell's proof of the first implication relies on partial results on the Birch–Swinnerton-Dyer conjecture due to Coates and Wiles.

References

[1] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae* **39** (1977), no. 3, 223–251.

[2] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics (2)* **141** (1995), no. 3, 553–572.

[3] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2. *Inventiones mathematicae* **72** (1983), 323–334.

[4] A. Wiles, Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics (2)* **141** (1995), no. 3, 443–551.